PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

DISERTACIÓN PREVIA A LA OBTENCION DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIÓN

TEMA:

"ESTUDIO COMPARATIVO DE SISTEMAS DE VIRTUALIZACIÓN Y DE SEGURIDAD. CASO DE ESTUDIO MUSEO QCAZ DE LA PUCE."

AUTOR: DAMIÁN ANÍBAL NICOLALDE RODRÍGUEZ

DIRECTOR: PHD, GUSTAVO CHAFLA

Quito – 2014

Índice

Índice i

Dedicatoria v

Agradecimiento vi

Introducción vii

Resumen ix

Objetivos x

Objetivo General: x

Objetivos Específicos: x

CAPÍTULO I 1

FUNDAMENTACIÓN TEÓRICA 1

1.1. Data Centers 1

1.1.1. Componentes de un Data Center 1

1.1.2. Objetivos del Data Center 2

1.1.3. Características del Data Center 3

1.1.4. Funciones del Data Center en la Empresa 4

1.1.5. Estándares para la implementación de un Data Center 5

1.1.6. Estándar TIA-942 Estándar de infraestructura de telecomunicaciones para Data Centers 7

1.1.7. Sistemas de cableado del Data Center 12

1.1.8. Uptime Institute 12

1.2. Virtualización 14

1.2.1. Servidor de virtualización (SerV) 15

1.2.2. Virtualización del almacenamiento (StoreV) 16

1.2.3. Virtualización de red (NetV) 17

1.2.4. Administración de la virtualización (ManageV) 17

1.2.5. Virtualización de escritorios (DeskV) 18
1.2.6. Virtualización de la presentación (PresentV) 18
1.2.7. Virtualización de aplicaciones (AppV) 18
1.2.8. ¿Qué es una máquina virtual? 18
1.2.8.1. Componentes de una máquina virtual (VM) 19
1.2.9. Modelos de virtualización de servidores 20
1.2.10. VMware 20
1.2.10.1. VMware vSphere 27
1.2.11. Microsoft Virtualization with Hyper-V 31
1.2.11.1. Hyper-V de Microsoft 33
1.3. Seguridad 36
1.3.1. ¿Qué es la seguridad? 36
1.3.2. Mitos de seguridad 37
1.3.3. Organismos que regulan la seguridad informática 38
1.3.4. Seguridad de redes de computadoras 38
1.3.4.1. La arquitectura de seguridad 39
1.3.5. Firewall 43
CAPÍTULO II 45
METODOLOGÍA 45
2. Metodología 45
2.1. Cómo diseñar un Data Center óptimo 45
2.1.1. Diseño Multidisciplinario 45
2.1.2. Áreas funcionales o espacios 45
2.1.3. Diagrama de distribución 46
2.1.4. Requerimientos de un Data Center 47
2.1.5. Mejores prácticas 49

2.1.6. Sistemas de cableado 49
2.1.6.1. Medios de transmisión 51
2.1.6.2. Racks y gabinetes 51
2.1.7. Consideraciones eléctricas 52
2.1.8. Consideraciones del sistema de enfriamiento 53
2.2. Análisis comparativo entre sistemas de virtualización 54
2.3. Diagnóstico del tráfico de la red del Museo QCAZ con Wireshark 57
2.3.1. Tipos de ataques a analizar 59
2.3.2. Análisis de MALWARE 64
2.3.3. Filtros 65
2.3.4. Análisis Follow TCP stream 66
2.3.5. Gráficos de Wireshark 69
2.4. Planificación e implementación de un Firewall 71
2.4.1. Plan 72
2.4.1.1. Vulnerabilidades de los sistemas de información 72
2.4.1.2. Pérdida de la confidencialidad, integridad y disponibilidad de los servicios 73
2.4.2. Configure 73
2.4.3. Test 73
2.4.4. Deploy 74
2.4.5. Manage 74
2.4.6. Implementación del Firewall en el Museo QCAZ 75
2.4.6.1. Configuración del firewall (Untagle) 75
2.4.6.2. Hardware y software a utilizarse 75
2.4.6.3. Políticas de seguridad 75
2.4.6.4. Red del Museo QCAZ 78

CAPÍTULO III 79
APLICACIONES 79
3. Aplicaciones 79
3.1. Instalación y configuración del sistema de virtualización con VMWare para el Museo QCAZ. 79
3.2. Instalación y configuración de los servidores para el Museo QCAZ 83
3.3. Instalación y configuración de un Network Gateway (pasarela de red). ..95
CAPÍTULO IV 100
CONCLUSIONES Y RECOMENDACIONES 100
4. Conclusiones y recomendaciones 100
4.1. Conclusiones 100
4.2. Recomendaciones 102
5. Literatura citada 103
ANEXOS 106
ANEXO 1 – Plan de Disertación 106
ANEXO 2 – Instalación paso a paso de VMware vSphere ESXi 5 120

Dedicatoria

Dedico el presente trabajo primero a Dios, quien inspiró mi mente para la conclusión del mismo. A mi esposa Patty y a mi hijo Marcos Damián quiénes siempre me alentaron a seguir y me brindaron todo el cariño del mundo, a mis padres Rosita y Aníbal quienes me dieron la vida, educación y consejos, a mis hermanos Daniel y Esteban quienes siempre me apoyaron, a mi director de tesis Gustavo quién me guió de inicio a fin y a Ramiro de quien siempre recibí palabras de aliento desde que inicie la maestría, lamentablemente no pudo estar presente para la culminación de la misma pero se que tu espíritu siempre estará aquí.

Agradecimiento

Primero quiero agradecer a la Pontificia Universidad Católica del Ecuador por haberme dado la oportunidad de prepararme. A mi director de tesis Doctor Gustavo Chafla por su dedicación, su tiempo, orientaciones y apoyo, a los Doctores Santiago Ron y Omar Torres por haberme facilitado la infraestructura del Museo QCAZ, a mis compañeros de maestría con quienes compartimos muchos momentos, a todos mis maestros quienes impartieron todos sus conocimientos y a toda mi familia.

Introducción

Un flujo ininterrumpido de innovaciones en el campo de las tecnologías de información, desde el internet hasta redes inalámbricas sigue transformando el mundo. Estas innovaciones están permitiendo la creación de nuevos productos y servicios tecnológicos como: compartir información, comunicaciones digitales, Tv digital. Muchos de estos nuevos productos y/o servicios corren sobre internet o están basados en la tecnología de internet.

Estos nuevos productos y/o servicios necesitan de una infeaestructura tecnológica actual, que pueda ofrecer un soporte adecuado de tal manera que se pueda brindar un servicio eficiente, se pueda garantizar disponibilidad y continuidad en las operaciones. Para cumplir con este objetivo las empresas han invertido mucho dinero para construir un ambiente apropiado y seguro en el cual se albergan todos los servidores, equipos de telecomunicaciones y los sistemas de almacenamiento. Estos ambientes conocidos como Data Centers son considerados como el centro nervioso de toda empresa, ya que están especialmente diseñados para soportar las necesidades de escalabilidad, redundancia, balanceo de carga, respaldo de energía y seguridad.

Los Data Centers, producto de decisiones poco planificadas o producto de un crecimiento mayor al esperado, han generado, que las organizaciones cuenten con una infraestructura demasiado grande, variada y dificil de administrar. En estos tiempos donde la disponibilidad, costo y eficiencia eléctrica son características importantes, han hecho pensar seriamente en migrar servicios a plataformas más eficientes y sólidas, que permitan reducir el tamaño de los Data Center en terminos de inventarios, costos y facilidad para administrarlos.

Una técnica empleada para reducir el tamaño de un Data Center es la virtualización, esto es que un solo recurso físico, como un servidor, aparezca como si fuera varios recursos lógicos a la vez. Esta técnica además permite subir el índice de utilización de los servidores a un 80 por ciento o más.

Un Data Center debe estar diseñado para bridar la seguridad de la información que se almacena en su graja de servidores, ya que cuya divulgación, alteración, pérdida o destrucción no autorizada puede producir daños imporantes a la organización propietaria de la misma. Es por esto que una de las tareas fundamentales de un Data Center es el área de seguridad. Para conseguir esto hay que facilitar las soluciones en continuidad, acceso, operación, procedimientos, con la finalidad de garantizar la disponibilidad en todo momento.

Resumen

Trabajo de investigación para aplicarse en la construcción de un Data Center óptimo, virtualización de servidores y políticas de seguridad de la información para el Museo QCAZ de la PUCE. Se utilizó el método científico que permitió revisar los conceptos, analizar el tráfico de la red del Museo y en base a los resultados tomar las mejores prácticas para implementarlas. Los materiales que se emplearon fueron: Vmware vSpher ESXi 5, Wireshark, Untangle, Microsoft Windows Server 2008 R2, servidor Hp ProLiant ML 350 G6, red virtual de pruebas, las técnicas aplicadas son: análisis de bibliografía, análisis de la red del Museo, pruebas de rendimiento de la red, pruebas de rendimiento del servidor.

Como resultado del presente trabajo se ha logrado la elaboración de una guía para el diseño y construcción de un data center óptimo basado en el estándar TIA-942, la implementación de una infraestructura virtualizada con VMware ESXi 5 y sobre este hypervisor la instalación de los servidores que permiten el correcto desempeño de las actividades del Museo (servidor web de producción y servidor de desarrollo, Network Gateway), y la instalación y configuración de una pasarela de red con Untangle, donde se realiza el filtrado del tráfico y el redireccionamiento de puertos. Esta infraestructura se encuentra instalada por seis meses, durante este tiempo se han realizado tareas de monitoreo de la red, rendimiento del servidor y se puede concluir que las técnicas utilizadas para el Museo son las más adecuadas ya que el rendimiento de la red y del servidor son óptimos.

La aplicación de una infraestructura virtualizada permite ahorro de recursos y aumentar la usabilidad de los servidores hasta un 80 por ciento, sin que el mismo se vea afectado en su rendimiento.

Se recomienda para el Museo la construcción de su propio Data Center de acuerdo a la guía desarrollada en el presente trabajo, con esto no se dependería de la infraestructura tecnológica de la universidad y de sus políticas de seguridad que muchas veces no permiten que las actividades del Museo se realicen eficientemente.

Objetivos

Objetivo General:

Realizar un estudio de Data Centers, sistemas de virtualización y seguridad que permita implementar un sistema de virtualización y seguridad en el Museo QCAZ de la PUCE.

Objetivos Específicos:

- Analizar los protocolos que permitan una adecuada implementación de una infraestructura de Data Center.
- Realizar un análisis entre los sistemas de virtualización más utilizados y determinar cuál es la opción más adecuada para implementarla en el Museo QCAZ.
- Instalar y configurar el ambiente virtual que permitirá la configuración de todos los servidores para el Museo QCAZ.
- Diagnosticar el tráfico de la red del Museo QCAZ de tal manera que se pueda diseñar las políticas de seguridad que se implementarán en el firewall.
- Instalar y configurar el firewall para el Data Center que permita gestionar y filtrar la totalidad del tráfico entrante y saliente de nuestra red, garantizando con esto la protección de los servidores en contra de accesos no deseados de intrusos que podrían ocasionar daños físicos y lógicos permitiendo asegurar la confidencialidad, integridad y disponibilidad de la información del Museo QCAZ.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

1.1. Data Centers

Los Data Centers albergan los recursos críticos de computación[1] en ambientes controlados y bajo una gestión centralizada (Arregoces & Portolani, 2004), lo que permite a las empresas garantizar una operación continua en sus actividades del negocio. Estos centros de datos deben tener la capacidad de administrar toda una gama de aplicaciones que se pueden encontrar en el mercado como: aplicaciones para fiscalización interna y de recursos humanos, e-commerce[2] y aplicaciones business-to-business. Además un número de servidores de apoyo para las operaciones de red y aplicaciones basadas en la red como: FTP[3], DNS[4], DHCP[5], TFTP[6], sistema de archivos de red NFS[7], aplicaciones para telefonía Ip, streaming de vídeo a través de Ip, etc.

1.1.1. Componentes de un Data Center

De acuerdo con (Barba & Viteri, 2012), los componentes de un Data Center son:

Espacio blanco: Es un espacio libre dentro del Data Center, necesario para tener la facilidad de reasignar tareas, funciones o equipos, es decir; un especio que permita crecer al Data Center o rediseñar su organización.

Infraestructura de apoyo: se refiere a los equipos adicionales que permiten que el Data Center garantice una operación continua en las actividades del negocio y además garantice la seguridad y protección de la información. Estos equipos son:

[1] Recursos de computación, incluyen mainframes, servidores web y de aplicaciones, servidores de archivos, de impresión, de mensajería, software de aplicación y sistemas operativos, además subsistemas de almacenamiento y la infraestructura de red.

[2] E-commerce: o comercio electrónico, consiste en la compra y venta de productos o servicio por medios electrónicos, ejemplo el internet.

[3] FTP: File Transfer Protocol (protocolo de trasferencia de archivos).

[4] DNS: Domain Name System (Sistema de nombres de dominio), su función es traducir las ips en nombres de dominio y viceversa.

[5] DHCP: Dynamic Host Configuration Protocol (protocolo de configuración dinámica de host), su función principal es asignar dinámicamente las direcciones ip con las configuraciones de la red.

[6] TFTP: Trivial File Transfer Protocol (protocolo de transferencia de archivos trivial)

[7] Sistemas de archivos de red NFS: permite a los hosts remotos montar sistemas de archivos sobre la red e interactuar con esos sistemas de archivos como si estuvieran montados localmente

transformadores, UPS[8], equipos de ventilación y aire acondicionado, panel de distribución de energía y equipos de transmisión remota.

Equipos de soporte: son los equipos que permiten una organización adecuada de los componentes del Data Center, como: racks[9], cableado estructurado, unidades de almacenamiento, equipos de red y además los equipos que permiten levantar los servicios que prestará el Data Center a la organización, estos son los servidores.

Operaciones: constituye el personal de operaciones o de soporte técnico, quienes aseguran que los equipos y la infraestructura tengan el mantenimiento adecuado y en caso de daños los reparen.

1.1.2. Objetivos del Data Center

Los beneficios proporcionados por un Data Center incluyen tradicionalmente objetivos orientados a los negocios; como el apoyo a las operaciones comerciales las 24 horas del día, todos los días del año, rebajando el costo total de operación y mantenimiento necesarios para sostener las funciones del negocio y el rápido despliegue de las aplicaciones y consolidación de los recursos de computación.

De acuerdo con (Arregoces & Portolani, 2004), estos objetivos orientados a los negocios generan una serie de iniciativas de Tecnologías de Información (TI), incluyendo las siguientes:

- Continuidad del negocio
- Incrementar la seguridad del Data Center
- Consolidar los servidores, aplicaciones y el Data Center
- Integrar aplicaciones de diferentes arquitecturas, ya sea cliente/servidor n capas, o aplicaciones web relacionadas con arquitectura orientada a servicios.

Estas iniciativas de TI son una combinación de las necesidades para hacer frente a problemas de corto plazo y establecer una dirección estratégica a largo plazo,

[8] El UPS es una pieza importante en la seguridad de los sistemas de información. Su principal tarea es tomar el control cuando ocurre una interrupción de energía eléctrica, dando a los usuarios el tiempo necesario para guardar sus trabajos en progreso.

[9] Un rack es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones

que permita al Data Center ser lo suficientemente flexible como para adaptarse a los cambios futuros. Los criterios de diseño son:

- Disponibilidad
- Escalabilidad
- Seguridad
- Rendimiento
- Capacidad de administración.

Estos criterios de diseño se aplican a las distintas áreas funcionales del Data Center, las cuáles son:

- **Servicios de infraestructura**: Rounting[10], switching y la arquitectura de la granja de servidores.
- **Servicios de aplicación**: balanceo de carga, Secure Socket Layer (SSL)[11], y el almacenamiento en caché.
- **Servicios de seguridad**: inspección y filtrado de paquetes, detección de intrusos.
- **Servicios de almacenamiento**: arquitectura SAN[12] (*Storage Area Network*), switching del canal de fibra, copias de seguridad y archivado.
- **Continuidad del negocio**: Extensión SAN, la selección del sitio y la interconectividad del Data Center.

1.1.3. Características del Data Center

Debido a que los Data Center albergan los recursos críticos de computación, las empresas deben hacer arreglos especiales tanto de las instalaciones y el personal necesarios para garantizar una operación 24-by-7.

Estas instalaciones soportan una alta concentración de recursos tecnológicos, servidores, infraestructura de red. Las demandas planteadas por estos recursos,

[10] Routing es el proceso que se realiza para determinar las tablas de encaminamiento por donde van a viajar los paquetes de datos.
[11] SSL (Secure Socket Layers) es un proceso que administra la seguridad de las transacciones que se realizan a través de Internet
[12] SAN es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía.

junto con la criticidad de las aplicaciones del negocio, crean la necesidad de abordar las siguientes áreas:

- Capacidad de potencia
- Capacidad de enfriamiento
- Cableado
- Controles de temperatura y humedad
- Sistemas de incendios y humo
- Seguridad física: sistemas de acceso restringido y vigilancia
- Espacios del rack y suelos falsos

1.1.4. Funciones del Data Center en la Empresa

La figura 1.1 presenta los diferentes bloques usados en la arquitectura de una red típica en una empresa, además ilustra la ubicación del Data Center dentro de esa arquitectura.

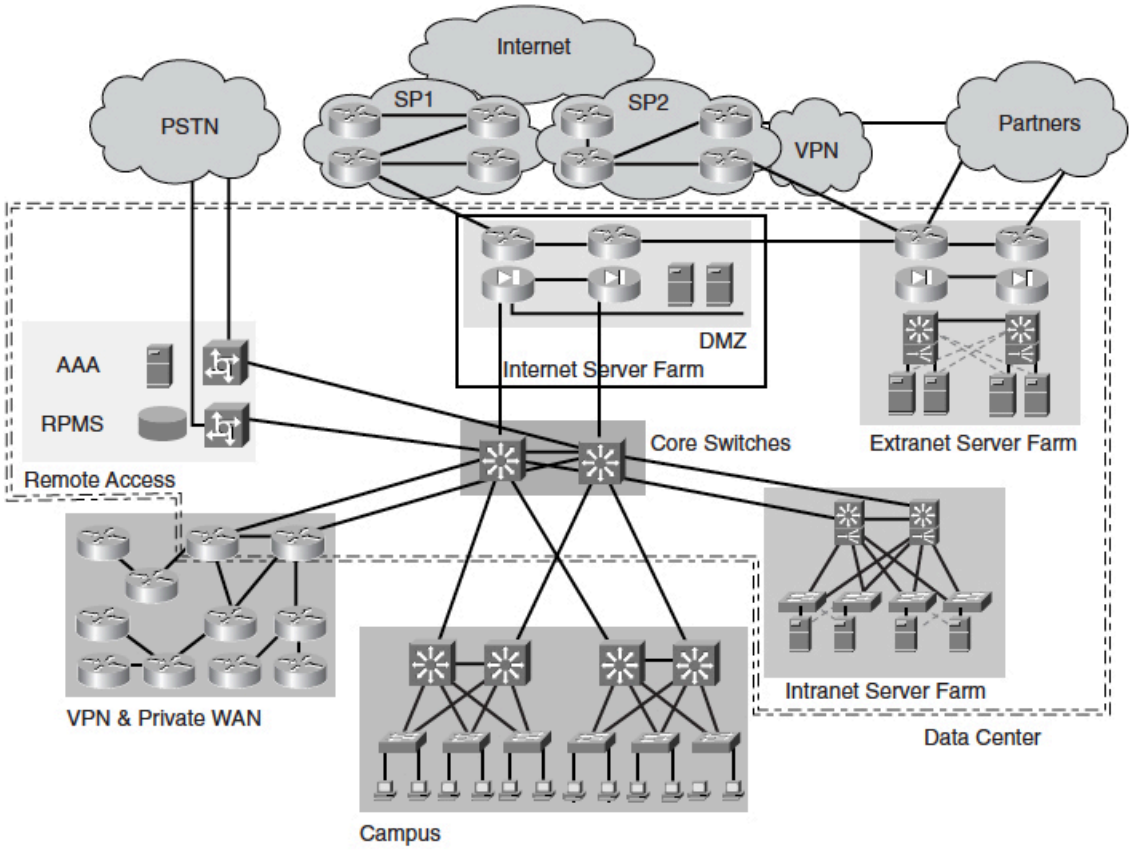


Figura 1.1 Data Center en la empresa, (Arregoces & Portolani, 2004)

Los bloques incluyen:

- Campus de la red
- Red privada - WAN
- Acceso remoto
- Granja de servidores de Internet
- Granja de servidores para la Extranet
- Granja de servidores para la Intranet.

Los Data Centers típicamente albergan muchos componentes, tales como los switches del campus de la red o los routers de borde de la red privada con la WAN. Los diseños de los Data Centers pueden incluir alguno o todos los bloques que se muestran en la Figura 1.1, incluyendo alguno o todos los tipos de granjas de servidores. Cada tipo de granja de servidores puede ser una entidad física independiente en función de los requerimientos de negocio de la empresa.

1.1.5. Estándares para la implementación de un Data Center

NFPA

NFPA 70 – Código Eléctrico Nacional[13]

Esta norma, permite verificar si las instalaciones eléctricas con las que cuenta la organización para el Data Center, cumplen los requerimientos mínimos aceptables para garantizar seguridad en los sistemas eléctricos. Además, establece como realizar una instalación segura de cableado eléctrico y equipos.

También conocido como NEC, es el punto de referencia para el diseño eléctrico seguro, la instalación y la inspección para proteger a las personas y bienes de los peligros eléctricos.[14]

NFPA 72 – Código de alarmas de incendio[15]

Establece la aplicación, instalación, ubicación, funcionamiento, inspección, prueba y mantenimiento de sistemas de alarmas contra incendios, equipos de alarma contra incendios y equipos de aviso de emergencia. Además del enfoque principal

[13] Extraído de: (Córdova, 2012)
[14] Extraído el 2 de junio del 2014 desde http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=70
[15] Extraído el 2 de junio del 2014 desde http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=72

en los sistemas de alarma de incendios, el Código incluye requisitos para los sistemas de notificación masiva utilizados para emergencias climáticas, eventos terroristas, biológicos, químicos y emergencias nucleares; y otras amenazas.

NFPA 75 – Protección de equipos electrónicos procesadores de datos por computadora[16]

Presenta un enfoque de la protección contra incendios y la continuidad del negocio basada en el riesgo. Para un negocio, el factor riego más importante es el que se ocasiona con la pérdida de información que se encuentra almacenada en las bases de datos de las organizaciones.

Este estándar cubre los requisitos para la protección de los equipos de tecnologías de información provocados por fuego o sus efectos asociados como: el humo, la corrosión, el calor y el agua.

NFPA 780 – Norma para la instalación de sistemas de protección contra rayos.[17]

Establece los requisitos de instalación del sistema de protección contra rayos, para proteger a las personas y bienes de los riesgos de incendios y peligros relacionados asociados con la exposición del rayo. Además en Córdova, D. 2012 se define un sistema de protección contra rayos como un sistema completo de terminales aéreas, conductores, terminales de conexión a tierra, conductores de interconexión, dispositivos de supresión de picos, y otros conectores o aditamentos requeridos para completar el sistema.

ANSI/TIA/EIA

ANSI/TIA/EIA 568-B Estándar de cableado de telecomunicaciones en edificios comerciales

- **TIA/EIA 568-B.1** Requerimientos generales
- **TIA/EIA 568-B.2** Componentes de cableado mediante par trenzado balanceado
- **TIA/EIA 568-B.3** Componentes de cableado, fibra óptica

[16] Extraído el 2 de junio del 2014 desde http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=75.
[17] Extraído el 2 de junio del 2014 desde http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=780

ANSI/TIA/EIA 569-A Normas de recorridos y espacios de telecomunicaciones en edificios comerciales, indica la forma en que se debe enrutar el cableado.

ANSI/TIA/EIA 570-A Normas de infraestructura residencial de telecomunicaciones.

ANSI/TIA/EIA 606-A Normas de administración de infraestructura de telecomunicaciones en edificios comerciales.

ANSI/TIA/EIA 607 Requerimientos para instalaciones de sistemas de puesta a tierra de telecomunicaciones en edificios comerciales.

ANSI/TIA/EIA 758 Norma cliente-propietario de cableado de planta externa de telecomunicaciones.

ANSI/EIA 310-D Establece las dimensiones de los racks y los define como un simple armazón metálico con un ancho normalizado de 19 pulgadas. El armazón cuenta con guías horizontales donde puede apoyarse el equipamiento, así como puntos de anclaje para los tornillos que fijan dicho equipamiento al armazón (Córdova, 2012).

1.1.6. Estándar TIA-942 Estándar de infraestructura de telecomunicaciones para Data Centers[18]

Estándar creado con la intención de unificar criterios en: el diseño e implementación de los Data Centers, añadiendo a estos la planificación de la instalación, el sistema de cableado estructurado y el diseño de la red (Barba & Viteri, 2012).

El estándar TIA-942 presenta dos criterios a considerar: de recomendaciones y de asesoramiento, estos se aplican a la protección, rendimiento, compatibilidad y administración de los requisitos mínimos aceptables que indica el estándar.

Unidades de medida

En la tabla 1.1 se muestran los acrónimos de las unidades de medida que se deben considerar en el Data Center.

[18] Extraído el 2 de junio del 2014 desde http://global.ihs.com/search_res.cfm?RID=TIA&INPUT_DOC_NUMBER=TIA-942

A	Amperio
°C	Grado Centígrado
°F	Grado Fahrenheit
Gb/s	Gigabit/segundo
Hz	Hertz
kb/s	Kilobit/segundo
kHz	Kilohercio
kVA	Kilo voltio amperio
kW	Kilovatio
Lbf	Libra-fuerza
MHz	Mega Hertz
µm	Micra

Tabla 1.1 Unidades de medida, (Barba & Viteri, 2012)

La TIA-942, es una norma de infraestructura de telecomunicaciones para Data Centers, que ofrece una orientación sobre el diagrama de distribución del Data Center. Según la norma un Data Center debe tener las siguientes áreas funcionales:

- Uno o más cuartos de entrada
- Un área de distribución principal (MDA, por sus siglas en inglés: main distribution area)
- Una o más áreas de distribución horizontal (HDA, por sus siglas en inglés: horizontal distrubution areas)
- Un área de distribución de zona (ZDA, por sus siglas en inglés: zone distribution area)
- Un área de distribución de equipos.

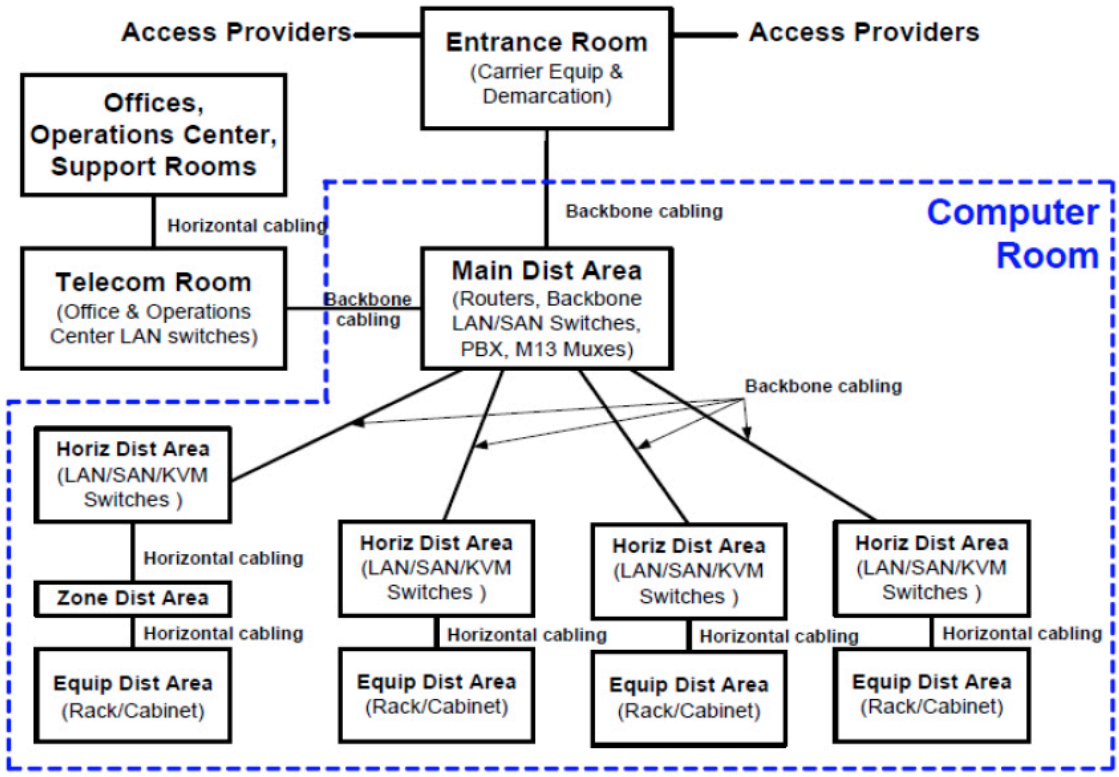


Figura 1.2 Ejemplo básico de un Data Center, (Barba & Viteri, 2012)

Cuarto de entrada

El cuarto de entrada alberga el equipo de los operadores de telefonía y el punto de marcación. Puede estar dentro del cuarto de cómputo, pero la norma recomienda que esté en un cuarto aparte por razones de seguridad. Si está ubicado en el cuarto de cómputo, deberá estar consolidado dentro del área de distribución principal.

Área de distribución principal

El área de distribución principal alberga el punto de conexión cruzada central para el sistema de cableado estructurado del Data Center. Esta área debe estar ubicada en una zona central para evitar superar las distancias del cableado recomendadas y puede contener una conexión cruzada horizontal para un área de distribución de un equipo adyacente. La norma especifica racks separados para los cables de fibra óptica, UTP y coaxial.

Área de distribución horizontal

El área de distribución horizontal es la ubicación de las interconexiones horizontales, el punto de distribución para el cableado hacia las áreas de distribución de los equipos. Puede haber una o más áreas de distribución horizontal, según el tamaño del centro de datos y las necesidades de cableado. Una directriz para un área de distribución horizontal especifica un máximo de 2000 cables UTP de 4 pares o terminaciones coaxiales (Barba & Viteri, 2012).

Área de distribución de zonas

Es el área de cableado estructurado para los equipos que van en el suelo y no pueden aceptar paneles de parcheo. Como ejemplo, se puede citar las computadoras centrales y algunos servidores.

Área de distribución de los equipos

Es la ubicación de los gabinetes y racks de equipos. La norma especifica que los gabinetes y racks se deben colocar en una configuración “hot aisle/cold aisle” (pasillo caliente / pasillo frío) para que disipen de manera eficaz el calor de los equipos electrónicos.

Requerimientos de los diferentes elementos de un Data Center (Córdova, 2012)

- Estructura
- Ubicación
- Acceso
- Protección contra incendios
- Equipos
- Redundancia

Distribución del Data Center (Córdova, 2012)

- Configuración de pasillos fríos y calientes
- Ubicación de gabinetes
- Láminas de piso falso
- Instalación de racks sobre piso falso

- Especificaciones

Configuración de pasillos fríos y calientes

Pasillos fríos. 1.0 a 1.2 metros

Pasillos calientes: 0.80 a 1.0 metros

Equipos y especificaciones (Córdova, 2012)

Gabinetes

- Altura máxima 2.4 metros, preferiblemente 2.1 metros.
- 42 U de espacio mínimo[19]
- profundidad de 1.0 a 1.1 metros
- Regletas: al menos una de 20 Amp/120V

Generador

- Alimentar los sistemas de aire acondicionado
- Instalar TVSS[20] (Transient Voltage Surge Supressors) en la salida
- Combustible, preferiblemente diesel, permite un arranque más rápido que con gas natural
- Sistema remoto de monitoreo y alarmas para el sistema de almacenaje de combustible.

Sistema UPS

- Suficiente tiempo de respaldo para que se encienda el generador
- Respaldo entre 5 a 30 minutos en baterías
- TIER 4 debe contar con un sistema Dual Bus con UPS redundantes
- El cuarto de UPS y baterías debe contar con un aire acondicionado de precisión (PAC)

[19] U: Unidad rack, es una unidad de medida usada para describir la altura del equipamiento preparado para ser montado en un rack de 19 ó 23 pulgadas de ancho. Una unidad rack equivale a 1,75 pulgadas (44.45 mm) de alto.

[20] TVSS: Los supresores de transitorios o dispositivos de protección contra sobretensiones transitorias (DPS) están conceptualizados por las normas internacionales como equipos destinados a proteger las instalaciones eléctricas contra aquellas sobretensiones (elevaciones de voltaje) generadas por fenómenos transitorios.

La finalidad principal de un Data Center es albergar los equipos y cableado, relacionados con los sistemas informáticos y sistemas de telecomunicaciones. Solo el personal autorizado tendrá acceso a esta sala.

Los parámetros de operación en el Data Center son:

- Temperatura entre 20 y 25 grados centígrados
- Humedad entre el 40 a 55 por ciento
- Tasa de oscilación de temperatura de 5 grados centígrados por hora.

1.1.7. Sistemas de cableado del Data Center

Cableado horizontal

Comprende al cableado que se extiende desde la sala de equipos hasta la sala de distribución principal. El cableado horizontal debe ser instalado en una topología de estrella, cada terminación en el área de distribución debe conectar a un equipo (Barba J. y Viteri G. 2012).

La distancia máxima del cableado horizontal no debe pasar los 90 metros, independientemente del tipo de equipos o medios de comunicación y 300 metros para fibra óptica.

Longitud (metros)	Área de cables (metros)	Área de cables, cables conexión (UTP) y equipos (metros)
90	5	10
85	9	14
80	13	18
75	17	22
70	22	27

Tabla 1.2 Tabla de longitud máxima de los cables en el cableado horizontal, (TIA, 2005)

Cableado vertical o Backbone

Este estándar recomienda y está certificado el uso del cable par trenzado categoría 6 de 100 ohm, fibra óptica multimodo 50/125 y fibra óptica monomodo 62.5/125

1.1.8. Uptime Institute

El Uptime Institute, Inc. es un consorcio de empresas dedicadas a la maximización de la eficiencia y el tiempo de actividad en los Data Centers y de las

organizaciones. Las empresas miembros aprenden unos de otros a través de reuniones patrocinadas, tours, redes y puntos de referencia.

El Uptime Institute ofrece varios servicios a sus miembros, incluyendo información anticipada sobre los productos y servicios que afectan a la disponibilidad, eficiencia y fiabilidad, las tendencias de tiempo de actividad y parámetros de la industria. Las normas de desempeño desarrolladas por el Instituto se basan únicamente en las necesidades y preferencias de los usuarios. La organización ofrece seminarios públicos y privados, ofrece sesiones de formación y lleva a cabo investigaciones patrocinadas. Desde 1993, el Instituto ha mantenido una red de miembros que aborda y busca soluciones para las cuestiones relativas a la refrigeración del centro de datos y los sistemas eléctricos.

Uptime Institute clasificó los siguientes aspectos para un Data Center: disponibilidad, confiabilidad, costos de construcción y mantenimiento del Data Center (Barba & Viteri, 2012).

El Uptime Institute ha definido un sistema de certificación (TIER) de Data Centers basado en cuatro niveles[21]:

- **TIER 1: Básico**, diseño mecánico y eléctrico de una sola ruta, sin componentes redundantes, disponibilidad 99.671%. El tiempo de construcción es aproximadamente de tres meses.
- **TIER 2: Componentes redundantes**, diseño mecánico y eléctrico de una sola ruta, con componentes redundantes, disponibilidad 99.741%. El tiempo de construcción es aproximadamente de tres a seis meses.
- **TIER 3: Mantenimiento concurrente**, diseño mecánico y eléctrico múltiple, pero solo una ruta activa, componentes redundantes, disponibilidad 99.982%. El tiempo de construcción es aproximadamente de quince a veinte meses.
- **TIER 4: Tolerante a fallas**, diseño mecánico y eléctrico múltiple, ambas rutas activas, componentes redundantes, disponibilidad 99.995%. El tiempo de construcción es aproximadamente de quince a veinte meses.

[21] Extraído de: (Córdova, 2012)

1.2. Virtualización

La virtualización en su forma más simple es la abstracción de hardware desde el software. Esta abstracción puede darse de diferentes formas. Esta puede ser en forma de virtualización del sistema operativo como: Hyper-V, virtualización de presentación con los servicios de terminal o virtualización de la aplicación con App-V, compañías como Cisco, Hp tienen sistemas de virtualización para la red y almacenamiento (Kappel, Velte, & Velte, 2009).

La virtualización del sistema operativo es la más popular hoy en día, esta no es solamente utilizada en los servidores, también se encuentra en las estaciones de trabajo para desarrollo y demostraciones.

La virtualización puede ayudar a las empresas a maximizar el valor de las inversiones de las Tecnologías de Información (TI), disminuyendo la huella del hardware de servidor, el consumo de energía, el costo y la complejidad de la administración de los sistemas de TI, al mismo tiempo que aumenta la flexibilidad del entorno general (Kappel et al., 2009).

En la actualidad la tecnología de la virtualización ha evolucionado y ahora se puede aplicar a varios niveles dentro del Data Center. En un Data Center que se aprovecha al máximo la propuesta de la virtualización habrá al menos siete capas de virtualización (ver la figura 1.3):

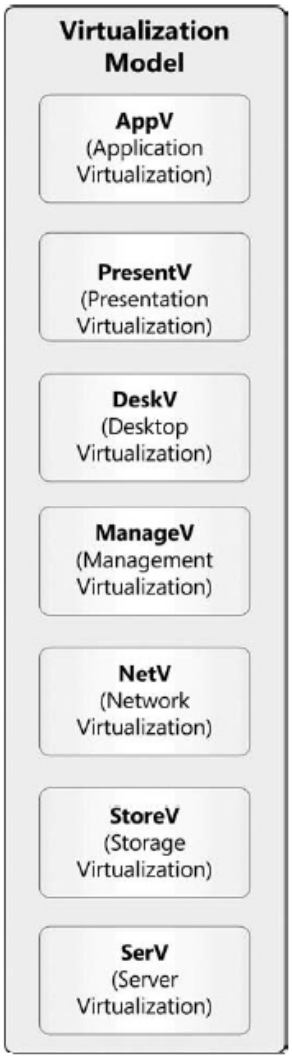


Figura 1.3 Los siete aspectos de la virtualización, (Ruest & Ruest, 2009)

1.2.1. Servidor de virtualización (SerV)

Se centra en la partición de una instancia física de un sistema operativo dentro de una instancia virtual o máquina virtual. Se debe considerar dos aspectos del servidor de virtualización:

Software de virtualización (SoftV): corre el sistema operativo virtualizado sobre una plataforma de software de virtualización que se ejecuta en un sistema operativo existente.

Hardware de virtualización (HardV): corre el sistema operativo virtualizado sobre una plataforma de software que se ejecuta directamente sobre el hardware sin un sistema operativo existente. El motor usado para correr la virtualización de

hardware es usualmente referido como hypervisor. El propósito de este motor es exponer a los recursos de hardware para los sistemas operativos virtualizados.

Cuando se trabaja con la virtualización de servidores, el servidor físico se convierte en el anfitrión para todos los sistemas operativos virtuales o máquinas virtuales (VMs) que se convierten en cargas de trabajo que se ejecutan sobre este host (Ruest & Ruest, 2009).

1.2.2. Virtualización del almacenamiento (StoreV)

El servidor de virtualización del almacenamiento se utiliza para combinar el almacenamiento físico de múltiples dispositivos de forma que aparezcan como una sola agrupación de almacenamiento, la misma puede tomar varias formas: almacenamiento de conexión directa (DAS), la red de almacenamiento (NAS), o redes de área de almacenamiento (SANs); y puede estar vinculado a través de varios protocolos: Fibre Channel, Internet SCSI (iSCSI), Fibre Channel on Ethernet, o incluso el Network File System (NFS).

Aunque la virtualización de almacenamiento no es un requisito para la virtualización de servidores, una de las fortalezas de la virtualización de almacenamiento es la capacidad de confiar en el “thin provisioning” o la asignación de una unidad lógica (LUN) de almacenamiento de un tamaño determinado. Por ejemplo: si se crea un LUN de 100 GB y sólo se utiliza 12 GB, los 12 GB de almacenamiento son los aprovisionados. Esto reduce el costo de almacenamiento (véase figura 1.4) (Ruest & Ruest, 2009).

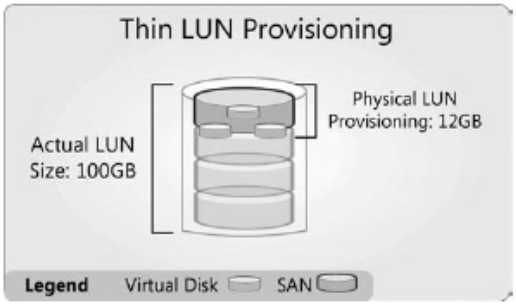


Figura 1.4 Thin LUN Provisioning, (Ruest & Ruest, 2009)

1.2.3. Virtualización de red (NetV)

La virtualización de red, permite controlar el ancho de banda disponible mediante la división del mismo en canales independientes que se pueden asignar a los recursos específicos.

Por ejemplo, la red área local virtual (VLAN), es un método para crear redes lógicas independientes dentro de una misma red física. Además, los productos de virtualización de servidores admiten la creación de capas de red virtual dentro del propio producto. Por ejemplo, el uso de esta capa de red virtual permitiría que se coloque una red perimetral en el mismo host, sin afectar las otras cargas de trabajo virtuales (Ruest & Ruest, 2009).

1.2.4. Administración de la virtualización (ManageV)

Se centra en las tecnologías que manejan todo el Data Center, tanto físico como virtual, con la finalidad de presentar una infraestructura unificada única para la prestación de los servicios.

ManageV no se realiza necesariamente a través de una sola interfaz. Por ejemplo, en los grandes Data Centers, se tendrá que dividir las diferentes prestaciones de servicios en capas y operaciones separadas entre ellas. En Data Centers más pequeños, generalmente no existe el personal suficiente para dividir las responsabilidades, pero al menos debe asegurarse que los administradores usen diferentes accesos cuando trabajan con las distintas capas de la arquitectura. Para la administración de la virtualización se debe asegurar de que las dos capas principales se cumplan en todo momento:

Resource Pools (RP), que incluye la recolección de recursos de hardware, servidores, racks, almacenamiento y hardware de red, que forman la infraestructura del Data Center.

Virtual Services Offerings (VSO), o cargas de trabajo que se componen de las máquinas virtuales (servidores, equipos de escritorio), que son los servicios de cara al cliente y servicios a usuarios finales.

Un factor clave para la administración de la virtualización es la creación de diferentes contextos de seguridad entre los recursos y los VSOs. Por ejemplo, la capa física debe utilizar contraseñas seguras y garantizar que todas las

comunicaciones entre las consolas de gestión y los hosts físicos se cifren en todo momento ya que las contraseñas se comunican a través de estos enlaces (Ruest & Ruest, 2009).

1.2.5. Virtualización de escritorios (DeskV)

Permite que las máquinas virtuales provisionen sistemas de escritorio. La virtualización de escritorio, tiene varias ventajas, una de las cuales es la capacidad de centralizar las implementaciones de escritorios y reducir los costos de gestión distribuidos ya que los usuarios acceden a los escritorios centralizados a través de una variedad de dispositivos delegados o no administrados (Ruest & Ruest, 2009).

1.2.6. Virtualización de la presentación (PresentV)

La virtualización de la presentación hasta hace poco llamados servicios de Terminal Server, proporciona la capa presentación desde una ubicación central para los usuarios. Aunque la necesidad de PresentV está disminuyendo debido a la introducción de tecnologías como la virtualización de aplicaciones, los protocolos utilizados para PresentV están a la vanguardia de las tecnologías DeskV y SerV, ya que son los protocolos utilizados para acceder, utilizar y administrar las cargas de trabajo virtuales (Ruest & Ruest, 2009).

1.2.7. Virtualización de aplicaciones (AppV)

Utiliza los mismos principios que SerV, pero en lugar de proporcionar un motor para ejecutar un sistema operativo, despliega las aplicaciones desde el sistema operativo a cualquier cliente virtual. Elimina la necesidad de instalaciones locales de las aplicaciones.

1.2.8. ¿Qué es una máquina virtual?

La virtualización es una tecnología que divide una computadora en varias máquinas independientes que pueden soportar diferentes sistemas operativos y aplicaciones que se ejecutan simultáneamente. La gran ventaja de la virtualización es que se puede aumentar el porcentaje de utilización de un servidor físico de un 10 por ciento a un 60 u 80 por ciento (Ruest & Ruest, 2009) cargándole múltiples máquinas virtuales.

El software Hypervisor se ejecuta directamente en el hardware del servidor y actúa como coordinador para administrar múltiples sistemas operativos en máquinas virtuales independientes. En esta situación, cada instancia de un sistema operativo se ejecuta en una máquina virtual, esta instancia se convierte en un entorno operativo denominada auto-contenido que se ejecuta sobre el Hypervisor y se comporta como si se tratara de un equipo independiente.

1.2.8.1. Componentes de una máquina virtual (VM)

Una máquina virtual está formada por los siguientes componentes[22]:

Archivo de configuración: es un archivo que contiene la información general de la máquina virtual como: cantidad de RAM, número de procesadores, el número y tipo de tarjetas de red (NIC), el número y tipo de discos virtuales para la máquina virtual. Cada vez que se crea una nueva máquina virtual, se crea un archivo de configuración de la máquina virtual, es decir un archivo que indica al software de virtualización, como asignar los recursos físicos del host a la máquina virtual.

Archivo(s) de disco duro: son los archivos que contienen toda la información que normalmente se encuentra dentro de un disco duro físico. Cada vez que se crea una nueva máquina virtual, el software de virtualización crea un disco duro virtual, es decir un archivo que actúa como un disco duro. Cuando se instala el sistema operativo en la máquina virtual, este quedará contenido en este archivo, cada máquina virtual puede contener varios archivos de disco.

Archivos de memoria: estos son archivos que contienen la información que está en la memoria de la máquina virtual en ejecución, y pueden enviarse al disco cuando la máquina virtual esté apagada.

Archivo de estado de la máquina virtual: al igual que las maquinas reales, la máquinas virtuales soportan modos de funcionamiento similares a la suspensión o hibernación. En términos de virtualización esto significa una pausa o suspensión, así como guardar el estado de la máquina. Cuando se suspende una máquina virtual, su estado de suspensión se guarda en este archivo.

Otros archivos: son los archivos que contienen los registros y otra información de la máquina virtual.

[22] Extraído de: (Ruest & Ruest, 2009)

1.2.9. Modelos de virtualización de servidores

Existen dos modelos de virtualización de servidores (ver figura 1.5).

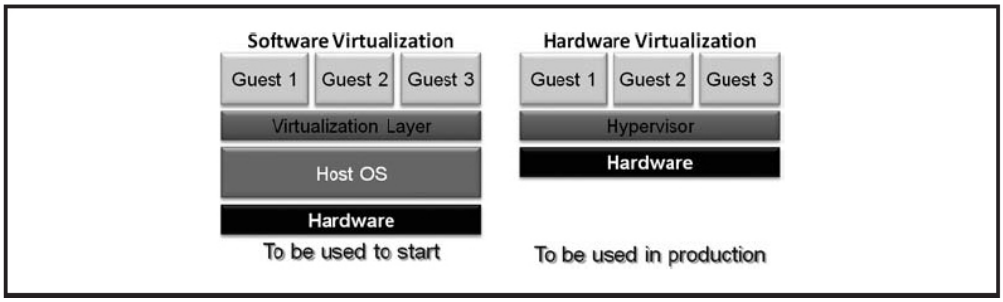


Figura 1.5 Modelos de virtualización de servidores, (Ruest & Ruest, 2009)

La primera, virtualización de software (SoftV), se utiliza a menudo para comenzar los proyectos de virtualización, se basa en las tecnologías más simples que generalmente son gratuitas. Es menos eficiente ya que requiere un sistema operativo host para ser instalada sobre este. Este sistema operativo también requiere recursos, debido a esto afecta el funcionamiento de las máquinas virtuales que se ejecutan sobre el mismo. Por esta razón este modelo se utiliza para pruebas o desarrollo.

El segundo modelo, virtualización de hardware (HardV), el Hypervisor se integra directamente con el hardware y simplemente expone el hardware del host a las máquinas virtuales que se ejecutan sobre este. El Hypervisor ocupa pocos recursos físicos del host, dejando la mayor cantidad para las máquinas virtuales que corren sobre él. Por esto, es el mejor modelo que se utiliza para la virtualización de servidores que son usados en producción.

1.2.10. VMware

En el año 2006, VMware lanza el concepto de Virtual Infrastructure, comienza la era de la infraestructura virtual. Este producto estaba basado en un Hypervisor muy robusto que ofrecía funcionalidades avanzadas de administración, alta disponibilidad y balanceo de carga que permitía correr aplicaciones críticas con una estabilidad muy alta.

El llamado Hypervisor es un componente de software que permite que varios sistemas operativos puedan acceder a un equipo en forma concurrente, como si

cada uno de ellos fuera el dueño coordinando el acceso y uso de sus recursos (ver Figura 1.6).

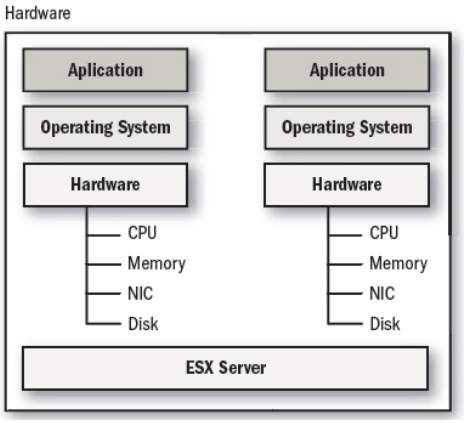


Figura 1.6. Hypervisor ESXi. (Marchionni & Formoso, 2012)

Para VMware el hypervisor es considerado como una capa intermedia entre el hardware y los sistemas operativos.

La clave del correcto funcionamiento de la infraestructura virtual es el almacenamiento centralizado. Todas las funcionalidades que ofrece VMware en su infraestructura virtual están basadas en un storage de discos. Para que la infraestructura virtual sea eficiente, altamente disponible y segura, esta debe contar con al menos un storage de discos en donde se almacenen y ejecuten las máquinas virtuales (ver figura 1.7).

VMware soporta NFS, ISCSI, Fiber Channel (FC) y Fiber Channel over Ethernet (FCoE) como protocolos de almacenamiento.

El espacio de almacenamiento que utiliza VMware se llama datastore y es parte del diseño de la solución, ya que su tamaño y la performance que brinda son clave para el funcionamiento de la infraestructura, el sistema de archivos usado es el VMFS[23] (Marchionni & Formoso, 2012).

[23] VMFS: Virtual Machine File System

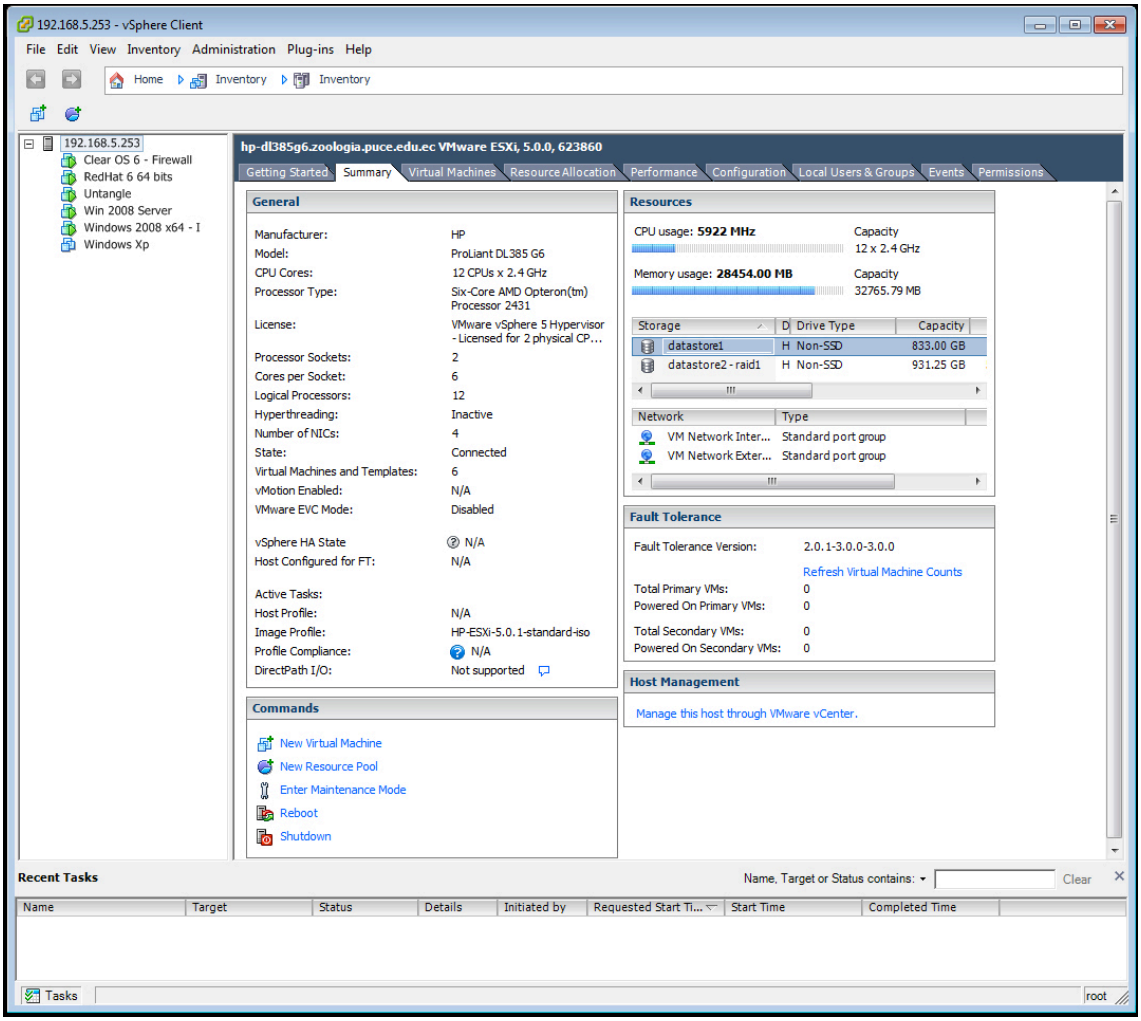


Figura 1.7. Resumen de un servidor virtualizado con VMware, (Nicolalde, 2014)

Análisis desde el punto de vista económico

Existen estadísticas en donde se indica que antes de la virtualización la tendencia de las organizaciones era comprar un servidor para cada aplicación o servicio, desperdiciando memoria, procesador y espacio en disco al punto de no llegar en la mayoría de los casos al 10 por ciento de uso e incluso menos (Marchionni & Formoso, 2012). El concepto de infraestructura virtual diseñado por VMware, permite resolver este problema. VMware utiliza servidores físicos con ESXi instalado, cuyo hypervisor tiene la capacidad de ejecutar múltiples instancias de máquinas virtuales y fue diseñado para aprovechar todos los recursos del servidor. Las mejores prácticas de VMware indican que el límite aceptable de consumo es de un 75 por ciento.

ESXi es la evolución del primer hypervisor para entornos abiertos de la industria que no depende de un sistema operativo para ejecutarse y fue desarrollado por VMware. De acuerdo con VMware, el EXSi es el hypervisor más liviano existente, ocupa aproximadamente 144 MB en disco.

Con VMware las tareas de mantenimiento son rápidas y muy fáciles de realizarlas, esto hace que las organizaciones logren una mejor inversión, y un menor costo en el mantenimiento y en la aplicación de mejoras.

En una infraestructura virtual con VMware la puesta en producción de un nuevo servidor no tarda más de 5 minutos, ya que no hay que seguir todos los trámites administrativos para comprar un nuevo equipo.

VMware generó una infraestructura virtual que es altamente disponible, logrando que cada máquina virtual esté protegida ante fallas de hardware o de software. Ante una caída de un ESXi o de una máquina virtual, el servicio de alta disponibilidad actúa de forma inmediata y automática para asegurar la continuidad del funcionamiento de la máquina o máquinas virtuales afectadas. La herramienta de alta disponibilidad es llamada HA.

VMware ha desarrollado un conector específico para el respaldo y recuperación de datos llamado VStorage API, este simplifica el proceso de respaldo dramáticamente. Además ha desarrollado una herramienta de respaldo Data Recovery sin ningún costo adicional. Con esto se logra eliminar el uso de agentes instalados en cada servidor y así generar una carga de trabajo excesiva que compita con las aplicaciones que son ejecutadas en ese momento, adicionalmente permite recuperar un equipo completo desde el mismo respaldo.

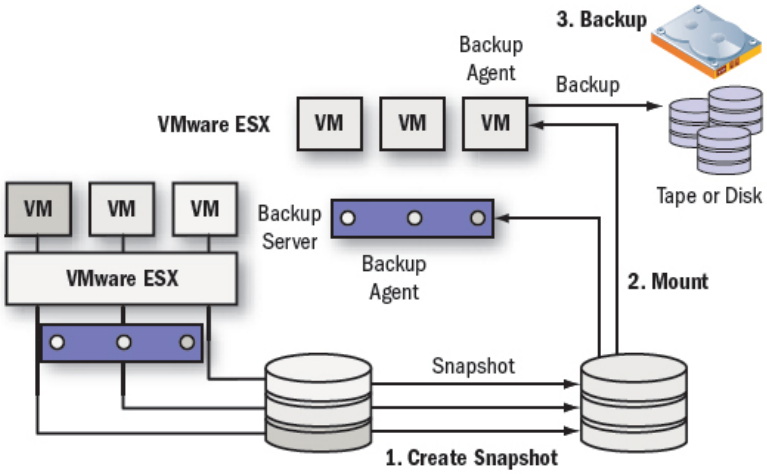


Figura 1.8. Esquema del funcionamiento del vStorage API, (Marchionni & Formoso, 2012)

Generar y mantener una solución de recuperación ante desastres resulta muy costoso. VMware en el año 2008 crea un producto que hasta hoy es único en el mercado Site Recovery Manager. Este producto que utiliza como base para su funcionamiento la infraestructura virtual de VMware (vSphere), automatiza el proceso de recuperación de las máquinas virtuales de un sitio en otro, en forma granular, y permite realizar pruebas de funcionamiento sin interrumpir el servicio (Marchionni & Formoso, 2012).

Análisis desde el punto de vista operativo

Las máquinas virtuales no dependen del hardware sobre el que se están ejecutando. Esto les permite moverse entre ESXis en tiempo real o por la falla de algún componente y que la infraestructura virtual escale en forma vertical, es decir, agregando mayor capacidad de procesamiento, o en forma horizontal, agrando más servidores a la infraestructura, sin que estos cambios generen una interrupción en el servicio. Existe otra característica que demuestra aún más la portabilidad de las máquinas virtuales el virtual appliance[24].

[24] Virtual appliance: es una máquina virtual que se encuentra preconfigurada de acuerdo a una funcionalidad específica que nos permite simplificar su puesta en marcha y administración. Actulamente existe un enlace (https://solutionexchange.vmware.com/store/category_groups/virtual-appliances) en la página de Vmware desde dónde se las puede descargar directamente.

La administración de la infraestructura en los entornos virtuales basados en vSphere es muy fácil de realizar, vCenter Server trae muchas herramientas que permiten realizar una administración centralizada (ver Figura 1.9).

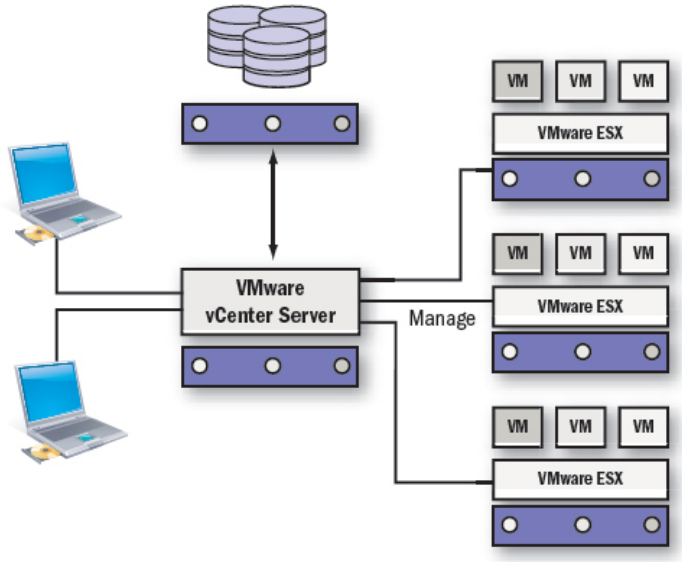


Figura 1.9. vCenter Server, (Marchionni & Formoso, 2012)

El vCenter Server permite la instalación automática de las actualizaciones a nivel ESXi, virtual appliances y las VMware Tools, monitoreo constante del hardware, monitoreo del rendimiento de la solución completa. Además, facilita la administración de la infraestructura virtual de una manera centralizada, simple y segura.

La infraestructura virtual permite que los administradores de los Data Centers puedan medir el nivel del crecimiento del consumo de los recursos de la infraestructura, de esta manera se puede calcular con suficiente anticipación el momento en que será necesario agregar más recursos. Con los informes de capacidad y tendencia de consumo que presente VMware, es más fácil darse cuenta cuando la capacidad virtual está llegando al máximo (en Figura 1.10 podemos observar la tendencia del consumo del CPU del nodo ESXi).

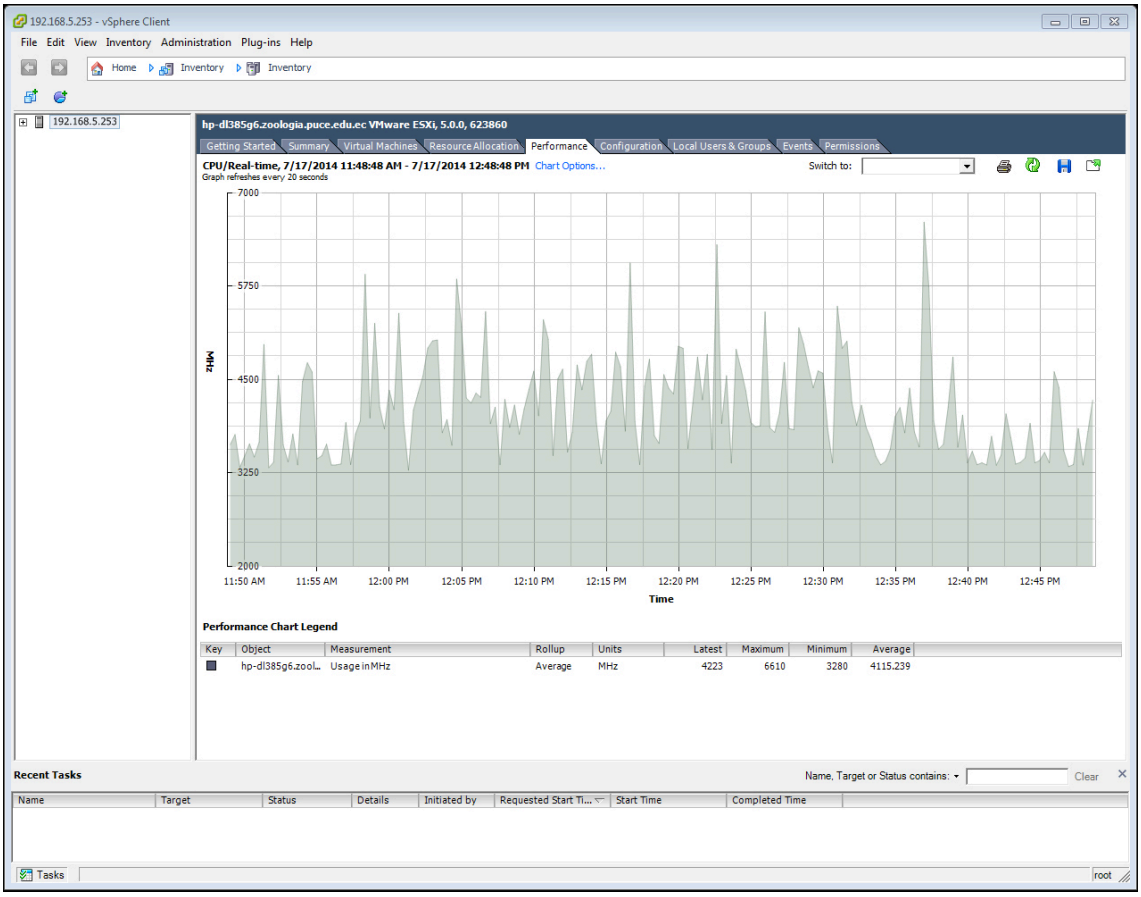


Figura 1.10. Tendencia de consumo del CPU, (Nicolalde, 2014)

La infraestructura creada por VMware está basada en la alta disponibilidad, logrando con esto que todas las máquinas virtuales funcionen de tal manera que se elimine el tiempo de parada de los servicios. Técnicas como HA (High Availability), Fault Tolerance[25], Update Manager, vMotion y DRS (Distributed Resource Scheduler) no solo evitan interrupciones no programadas, sino que pueden eliminar los tiempos de parada programados para tareas de mantenimiento.

Toda infraestructura debe ser escalable, es decir; debe adaptarse con facilidad a nuevos escenarios, elevar su calidad de servicio y expandir sus capacidades. En una infraestructura virtual la escalabilidad se puede hacer de varias formas, y en todas ellas, sin impacto al sistema operativo ni a las aplicaciones de las máquinas virtuales. Se puede agregar la capacidad de procesamiento, memoria y

[25] Fault Tolerance: esta funcionalidad eleva al máximo el nivel de disponibilidad de una máquina virtual generando una copia en tiempo real que queda oculta, si la máquina virtual productiva falla, la copia entra en funcionamiento en forma transparente y sin interrupción de servicio.

almacenamiento a cada ESXi, agregar nuevos ESXis, etc., sin que esto obligue a parar los servicios que se ejecutan en el entorno mencionado (Marchionni & Formoso, 2012).

1.2.10.1. VMware vSphere

Es una plataforma de virtualización a nivel de centro de datos, desarrollada por VMware. VMware vSphere es la plataforma de virtualización líder del sector para construir infraestructuras en la cloud. Permite a los usuarios ejecutar aplicaciones críticas para el negocio con confianza y responder con mayor rapidez a las necesidades empresariales. Con más de 250 000 clientes en todo el mundo y el respaldo de más de 2500 aplicaciones de más de 1400 partners ISV, VMware vSphere es la plataforma de confianza para cualquier aplicación (Tomado de VMware, http://www.vmware.com/files/es/pdf/VMware-vSphere-Standard-Edition-Datasheet.pdf, accedido el 18 de jul. de 2014). Esta plataforma esta basada en la capacidad de la solución para estar disponible continuamente, poder adaptarse a los cambios del negocio y lograr automáticamente la utilización balaceada de los recursos disponibles. HA, vMotion y DRS son las funcionalidades que ayudan para que estas premisas se cumplan (Marchionni & Formoso, 2012) (ver Figura 1.11).

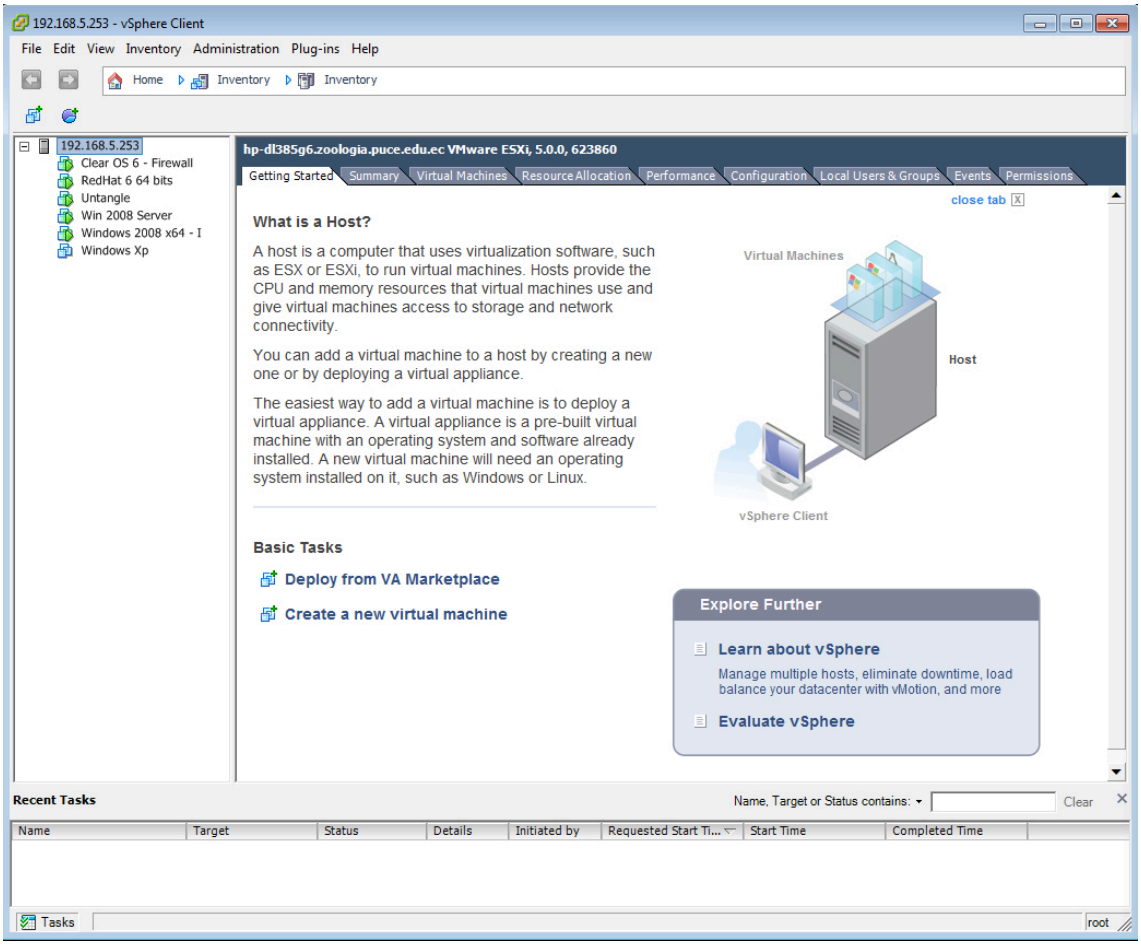


Figura 1.11. Consola central de VMware vSphere. Permite administrar toda la infraestructura virtual, (Nicolalde, 2014)

HA (High Availability/Alta Disponibilidad)

Es la solución automatizada más rentable para el reinicio de todas las aplicaciones y servicios en cuestión de minutos en caso de un fallo de hardware o del sistema operativo (Tomado de VMware, http://www.vmware.com/files/es/pdf/VMware-vSphere-Standard-Edition-Datasheet.pdf, accedido el 18 de jul. de 2014).

Esta función se habilita desde el vCenter a nivel de clúster[26]. La funcionalidad HA, cuando un ESXi queda fuera de servicio en forma inesperada, permite que las máquinas virtuales que son afectadas se reinicien en forma automática en los ESXis restantes y en base a la prioridad establecida para cada una (Marchionni & Formoso, 2012). En la Figura 1.12 se puede apreciar lo mencionado antes.

[26] Cluster: un cluster para vSphere es una agrupación lógica de ESXis que comparten las mismas funcionalidades y recursos.

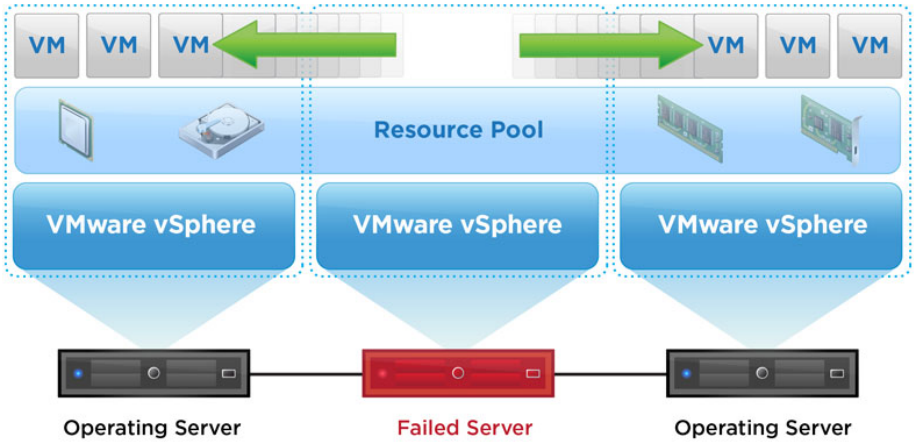


Figura 1.12. HA (High Availability/Alta Disponibilidad), http://www.yellow-bricks.com/vmware-high-availability-deepdiv/.

vMotion

Las migraciones en caliente con VMware vSphere® vMotion, permiten trasladar una máquina virtual completa y en funcionamiento de un servidor físico a otro, sin tiempo de inactividad. La máquina virtual retiene su identidad y conexiones de red, con lo que se garantiza un proceso de migración sin ningún tipo de problema. La memoria activa y el estado de ejecución preciso de la máquina virtual se transfieren a través de una red de alta velocidad, lo que permite que la máquina virtual pase de ejecutarse en el host de vSphere de origen a ejecutarse en el host de vSphere de destino. Todo este proceso tarda menos de dos segundos en una red Gigabit Ethernet (Tomado de VMware, http://www.vmware.com/es/products/vsphere/features/vmotion.html, accedido el 18 de jul. de 2014).

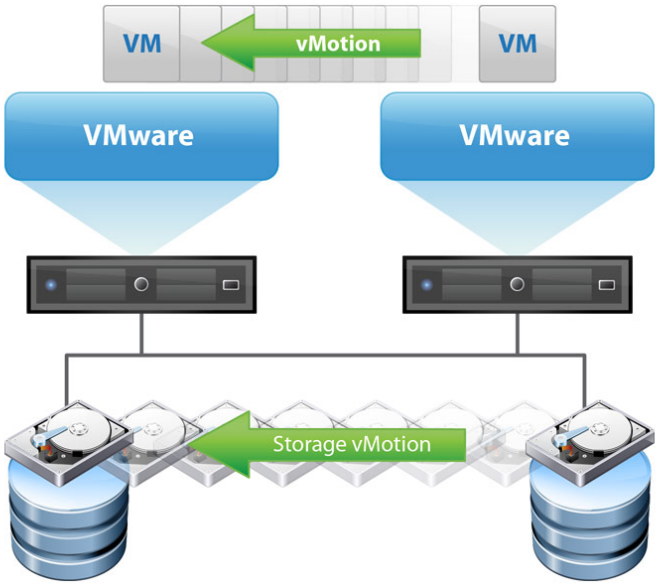


Figura 1.13. Concepto de la herramienta vMotion, http://www.vmware.com/es/products/vsphere/features/vmotion.html

DRS (Distributed Resource Scheduler - Programación de recursos distribuidos)

Esta funcionalidad logra utilizar equilibradamente los recursos entre los ESXis de un mismo clúster. Con DRS es posible crear resource pools, que permiten agrupar un conjunto de máquinas virtuales aplicando prioridades de uso de los recursos de procesamiento, memoria y acceso a disco, con el fin de establecer una jerarquía en caso de que estos recursos sean escasos (ver Figura 1.14).

Una funcionalidad adicional que se desprende de DRS es DPM (Distributed Power Management/Administración distribuida de energía). Cuando DMP está activado y se detecta que los recursos utilizados en el clúster pueden ser cubiertos por menos nodos que los que están en funcionamiento, de manera automática asigna las máquinas virtuales que estaban funcionando al resto de nodos utilizando DRS y luego apaga él o los nodos sobrantes. Cuando el nivel de consumo lo requiere, DPM vuelve a prender él o los nodos y balacea el consumo de recursos nuevamente (Marchionni & Formoso, 2012).

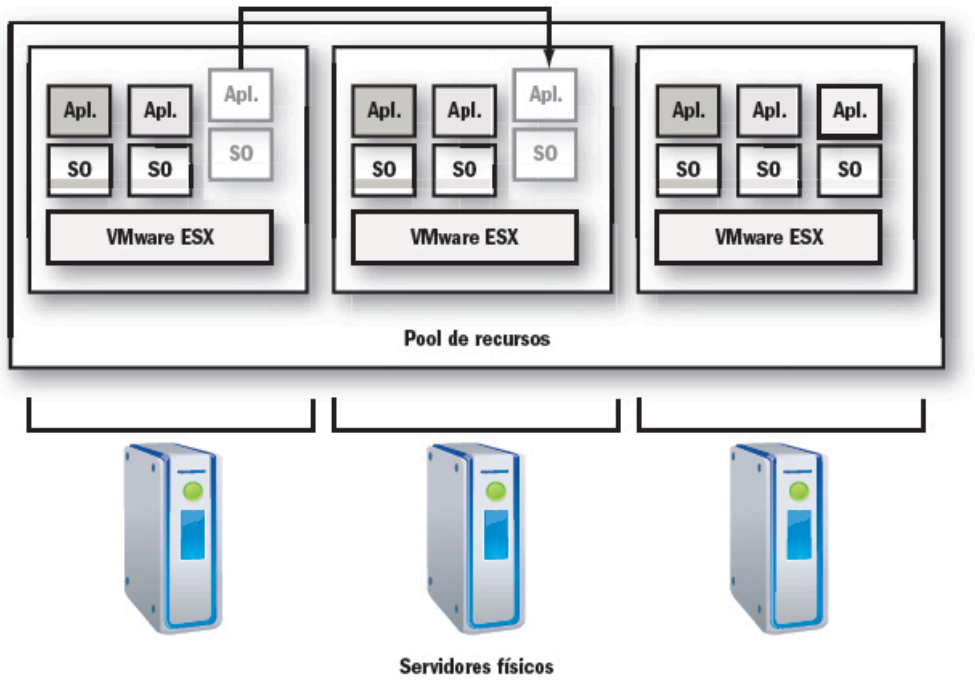


Figura 1.14. DRS, (Marchionni & Formoso, 2012)

1.2.11. Microsoft Virtualization with Hyper-V

En Windows Server 2012 R2 y System Center 2012 R2 Virtual Machine Manager, Microsoft ofrece una solución de virtualización de red completa. Existen cuatro componentes principales[27]:

- **Windows Azure Pack for Windows Server** proporciona un portal para inquilinos dirigido a la creación de redes virtuales.
- **System Center 2012 R2 Virtual Machine Manager (VMM)** proporciona servicios de administración centralizada de las redes virtuales.
- **Hyper-V Network Virtualization** proporciona la infraestructura necesaria para virtualizar el tráfico de red.
- **Hyper-V Network Virtualization Gateways** proporciona conexiones entre redes virtuales y físicas.

Windows Server 2012 es un sistema operativo totalmente especializado en el manejo de virtualización y conexión a la nube o Cloud Computing.

[27] Tomado de: http://technet.microsoft.com/es-es/library/jj134230.aspx, accedido el 7 de octubre de 2014

Con la virtualización, en un servidor físico se pueden instalar varios servidores virtuales, está única máquina física puede funcionar en la red como si fueran cuatro computadoras.

Con el paso del tiempo los administradores de sistemas se han dado cuenta que es más económico y provechoso usar los servidores virtuales, ya que estos brindan movilidad, economía, fácil acceso y a la abstracción de la computadora (Hypervisor), que crea una capa de abstracción entre en hardware de la máquina física y el sistema operativo de la máquina virtual.

Microsoft Hyper – V es el software de virtualización (manejador de máquinas virtuales) que trae Microsoft Windows Server 2012.

La arquitecta de los componentes de Hyper-V se divide en cuatro partes fundamentales:

- **Secure multitenancy** (Aislamiento seguro) se utiliza para mantener las máquinas virtuales aisladas dentro del mismo servidor siempre que estén en un mismo disco duro.
- **Flexible infrastructure** (Infraestructura flexible) permite la perfecta gestión de la red virtualizada, con Hyper-V se puede escalar más allá de lo que son las redes virtuales.
- **Scalability, performance and density** (escalabilidad, performance y densidad) escalabilidad soporta hasta 64 procesadores y 1TB de memoria para sistemas operativos, capacidad de disco que soporta hasta 64TB por disco virtual y proporciona flexibilidad para que se pueda virtualizar a gran escala.
- **High availability** (alta disponibilidad) las máquinas virtuales deben estar disponibles cuando se las necesite, Windows Server 2012 tiene soporte de hasta 4000 máquinas virtuales en paralelo.

Microsoft System Center (MSC)

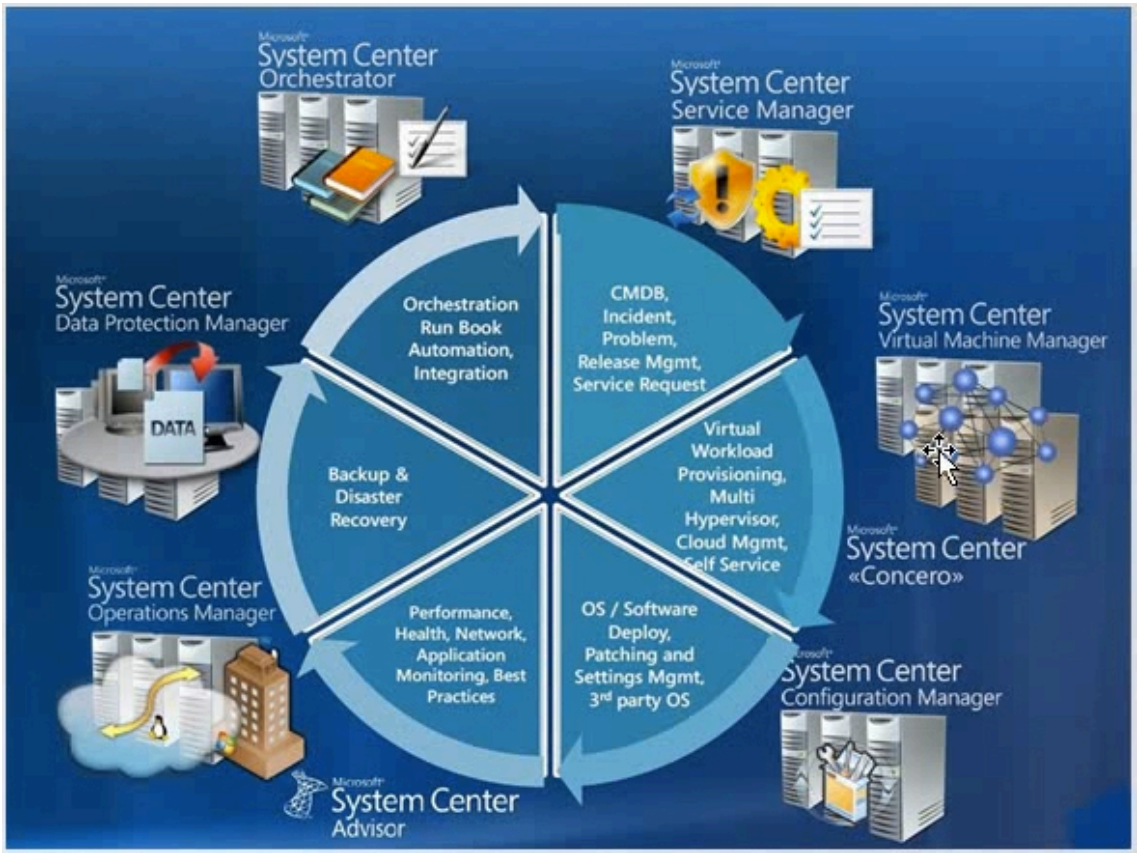


Figura 1.15. Microsoft System Center, Capacity Information Technology Academy, Microsoft Windows Server 2012. 2013

Es un conjunto de aplicaciones desarrolladas por Microsoft para la gestión de los diferentes componentes de la infraestructura informática de la organización. Es utilizado para controlar el rendimiento y la disponibilidad de equipos y sistemas, gestionar la instalación de actualizaciones de software, administrar el entorno de máquinas virtuales y elaborar informes para un correcto planeamiento que contribuya a optimizar las operaciones.

1.2.11.1. Hyper-V de Microsoft

De acuerdo a Microsoft Hyper-V es un programa de virtualización basado en un Hypervisor para sistemas de 64 bits. Para instalar Hyper-V y que funcione de manera eficiente se necesita: procesador de 64 bits, virtualización asistida por hardware (para Intel IntelVT Intel Virtualization Technology y para AMD

AMDVirtualization AMD-V), DEP[28] habilitado (Prevención de Ejecución de Datos) implementada por hardware.

Mejoras de Hyper-V en Windows Server 2012

- **Cliente Hyper-V**. Permite usar Hyper-V sin instalar un sistema operativo de servidor; es decir, está disponible para versiones de sistemas operativos de escritorio de Windows.
- **Memoria dinámica.** Se puede configurar memoria mínima y la paginación inteligente, que es una técnica de administración de la memoria que proporciona una experiencia de reinicio confiable en las máquinas virtuales configuradas con menos memoria mínima que la memoria de inicio. La paginación inteligente reduce el riego de que una máquina virtual no pueda reiniciarse si no hay suficiente memoria física disponible, para esto la paginación inteligente usa recursos de disco como memoria temporal extra cuando la máquina virtual requiere una mayor cantidad de memoria que la que tiene asignada.
- **Modulo Hyper-V para PowerShell.** Incluye más de 160 de cmdlets (comandos) que permiten administrar el Hyper-V, máquinas virtuales y discos duros virtuales de mejor manera y con mayor facilidad, esta característica permite replicar máquinas virtuales entre sistemas operativos de almacenamiento, clúster y centro de datos ubicados en dos sitios.
- **Réplica de Hyper-V.** Permite replicar máquinas virtuales entre sistemas de almacenamiento, clústeres y centros de datos ubicados en dos sitios para garantizar continuidad en el negocio y recuperación ante desastres.
- **Importación de máquinas virtuales.** El proceso de importación se ha simplificado y es más confiable. Ahora detecta ciertos problemas de configuración y ayuda a corregirlos de modo que la importación siempre se pueda realizar.

[28] Tomado de Microsoft. DEP: La Prevención de ejecución de datos (DEP **Data Execution Prevention**) es una característica de seguridad que ayuda a impedir daños en el equipo producidos por virus y otras amenazas a la seguridad. Los programas perjudiciales pueden intentar atacar Windows mediante la ejecución de código desde ubicaciones de la memoria del sistema reservadas para Windows y otros programas autorizados. Estos tipos de ataques pueden dañar los programas y los archivos.

- **Migración en vivo.** Es posible ejecutar una migración en vivo en un entorno no organizado en clústeres, esta migración se admite tanto si el almacenamiento se conserva en un recurso compartido central SMB o local, además ejecutar más de una migración al mismo tiempo y usar mayores anchos de banda de red (de hasta 10 Gigabits).
- **Medición de recursos.** Se puede conocer el uso de lo recursos de cada máquina virtual y obtener un reporte de esto.
- **Escala significativamente mayor y resistencia mejorada.** Hyper-V ofrece recursos de cálculo y almacenamiento significativamente más grandes que antes y mejora el tratamiento de los errores de hardware. Con esta característica se puede garantizar que Hyper-V, permite configurar máquinas virtuales grandes y de alto rendimiento que admitan cargas de trabajo que podrían necesitar escalarse verticalmente de manera significativa.

  El equipo en el que se ejecuta Hyper-V con Windows Server 2012 puede configurarse hasta con 320 procesadores lógicos y 4 TB de memoria. Cada máquina virtual puede configurarse hasta con 64 procesadores virtuales y 1TB de memoria.
- **Autorización simplificada.** Incluye un grupo local de administradores de Hyper-V, estos tienen acceso completo y sin restricciones a todas las características de Hyper-V.
- **SR-IOV.** Esta característica permite asignar un adaptador de red que admite la virtualización de E/S de raíz única (SR-IOV) directamente a la máquina virtual. Esto dispara el rendimiento de la red y reduce su latencia, así como la sobrecarga de CPU necesaria para procesar el tráfico de la red.
- **Migración de almacenamiento.** Mueve los discos duros virtuales que usa una máquina virtual a un almacenamiento físico diferente, mientras la máquina virtual sigue ejecutándose (en caliente).
- **Almacenamiento en recursos compartidos de archivos SMB 3.0.** Hyper-V admite el uso de recursos compartidos de archivos SMB 3.0 para proporcionar almacenamiento compartido para las máquinas virtuales sin una red de área de almacenamiento (SAN).

- **Canal de Fibra Virtual.** Permite establecer una conexión directa con el almacenamiento del canal de fibra desde el sistema operativo invitado que se ejecuta en una máquina virtual.
- **Formato del disco duro virtual.** El nuevo formato del disco duro virtual (VHDX) aprovecha las ventajas del nuevo hardware de almacenamiento. Admite hasta 64 TB de almacenamiento.
- **Instantáneas de máquinas virtuales.** Cuando una instantánea de máquina virtual se elimina, el espacio de almacenamiento que esta consumía antes de eliminarse, se recupera y vuelve a estar disponible mientras la máquina virtual se ejecuta.

Texto tomado de: Microsoft. 2012. http://technet.microsoft.com/es-es/library/hh831410.aspx, accedido el 28 de agosto de 2014

1.3. Seguridad

1.3.1. ¿Qué es la seguridad?

Los requerimientos de seguridad que involucran las tecnologías de información y comunicación, en pocos años han cobrado un gran auge, y más aún con el internet y en particular con todos los servicios relacionados con la web. Situación que ha llevado a la aparición de nuevas amenazas en los sistemas computarizados. De esta manera las políticas de seguridad emergen como el instrumento para concientizar a los miembros de las instituciones acerca de la importancia y sensibilidad de la información (Vogelmann Martínez, 2008).

El principal problema con la seguridad en las tecnologías de información y comunicación es que vivimos en una sociedad de información donde esta representa poder. Sin embargo, los altos directivos de las organizaciones aún no conceptualizan de manera adecuada la importancia de la seguridad de la información. Por ejemplo, en México el 30 por ciento de los encargados de seguridad informática nunca se reúnen con los altos directivos para hablar del aseguramiento de la información (Olivares Rojas, 2009).

La seguridad se está convirtiendo en uno de los principales problemas para el desarrollo de nuevas tecnologías. Los hackers están en constante evolución hacia

nuevas técnicas de ataque, por lo que la tarea de construir mecanismos de defensa se convierte en una misión difícil.

La comunidad de investigación siempre esta desarrollando modelos de seguridad destinados a derrotar los ataques. El ciclo es casi siempre el mismo: cada vez que una nueva técnica de ataque o vulnerabilidad de la red es descubierta por un investigador, este construye una técnica en concepto, que luego es evaluada y desarrollada (Awad & Hassanien, 2013).

La seguridad se refiere a la protección de la información (datos), de daño intencionado o accidental.

De acuerdo a (Olivares Rojas, 2009) los requisitos básicos de seguridad en las tecnologías de información y comunicación son:

- Autenticación
- Control de acceso
- Confidencialidad
- Integridad
- No repudio
- Disponibilidad
- Privacidad

1.3.2. Mitos de seguridad

Los principales mitos de la seguridad en las tecnologías de información y comunicación son:

- Ya compramos un firewall, ya existe seguridad. La respuesta es No
- Nunca ha pasado nada
- No se conecta a internet, no necesita seguridad
- Los empleados son de confianza
- Ver el problema de seguridad como un problema netamente tecnológico

Des acuerdo con (Olivares Rojas, 2009), algunas estadísticas en cuestión de problemas de seguridad son:

- El 32 por ciento de la pérdida de datos es causada por errores humanos
- El 25 por ciento de la pérdida de datos se deben a fallas físicas

- El 15 por ciento de la pérdida de datos el por la pérdida o robo de la información

A la seguridad se la debe considerar una inversión y no un gasto. Es cierto que la seguridad es costosa, pero es más costosa la inseguridad.

La seguridad en las tecnologías de información y comunicación, no solo afecta a recursos computacionales, sino, a la información de la empresa en general, esta puede ser:

- Información que se encuentra en base de datos, archivos, conocimiento de las personas.
- Documentos: contratos, manuales, facturas, solicitudes de crédito.
- Software: aplicaciones, sistemas operativos, utilitarios.
- Físicos: equipos, edificios, redes.
- Recursos humanos: empelados internos y externos.

1.3.3. Organismos que regulan la seguridad informática

Existen algunas organizaciones encargadas de la seguridad informática, las principales son: ISO (International Organization for Standardization), IEEE (Institute of Electrical and Electronics Engineers), ACM (Association for Computing Machinery), ISACA (Information System Audit and Control Association), ALSI (Academia Latinoamericana de Seguridad Informática). Estos organismos se encargan de regular los estándares, metodologías, guías base, etc., en cuestión de seguridad informática.

1.3.4. Seguridad de redes de computadoras

En esta era de la conectividad electrónica universal, de virus y hackers, de escuchas y de fraudes electrónicos, no hay un momento en el que no importe la seguridad. Con este antecedente de acuerdo a Cisco el modelo de seguridad de las empresas debe verse en todo su conjunto y considerar además de la red, dispositivos móviles, puntos terminales, ambientes virtuales y la nube.

Cisco indica que hay que buscar una solución de seguridad inteligente que permita protegerse antes, durante y después de un ataque.

Antes: deben existir políticas de acceso y conocimiento de lo que se encuentra en la red para monitorearlos y prevenir las amenazas.

Durante: se debe detectar la amenaza, bloquearla y defenderse de manera rápida y eficaz.

Después: hay que evaluar el daño, remediarlo y regresar a las operaciones normales lo antes posible.

De acuerdo a (Stallings, W. 2004) las necesidades de seguridad de la información en una organización han sufrido dos cambios fundamentales en las dos ultimas décadas. La primera con la introducción del computador, se hizo evidente la necesidad de proteger los archivos y otros tipos de información almacenada en el computador. Esto ocurre especialmente en el caso de sistemas compartidos, donde la necesidad se acentúa en sistemas a los que se puede acceder por medio de una red telefónica pública, una red de datos o internet.

El segundo cambio fue la introducción de sistemas distribuidos y el uso de redes y herramientas de comunicación para transportar datos entre el usuario de un terminal y el computador, y entre dos computadores. Las medidas de seguridad son necesarias para proteger la información durante la transmisión.

1.3.4.1. La arquitectura de seguridad

A continuación se describe el modelo de referencia básico que el CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) lo ha tomado para la Recomendación X.800 y su enmienda 1.

El CCITT es un órgano permanente de la Unión Internacional de Telecomunicaciones (UIT).

Recomendación X.800

Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.

El objetivo de la ISA (Interconexión de Sistemas abiertos) es permitir la interconexión de sistemas de computador heterogéneos de modo que puedan lograrse comunicaciones útiles entre procesos de aplicación. En distintos momentos, deben establecerse controles de seguridad para proteger la

información intercambiada entre los procesos de aplicación. Estos controles deben hacer que el costo de obtener o modificar los datos de una manera indebida sea mayor que el valor potencial de esta acción, o hacer que el tiempo requerido para obtener los datos de una manera indebida sea tan largo que pierdan su valor.

Servicios de seguridad

Se considera que los siguientes servicios de seguridad pueden proporcionarse facultativamente en el marco del modelo de referencia de ISA.

- Autenticación: proporcionan la autenticación de una entidad par comunicante y de la fuente de datos.
    - Autenticación de entidad par: cuando este servicio, es proporcionado por la capa (N), corrobora a la entidad (N+1) que la entidad par es la entidad (N+1) pretendida.
    - Autenticación del origen de datos: este servicio, cuando es prestado por la capa (N), corrobora a una entidad (N+1) que la fuente de los datos es la entidad par (N+1) pretendida.
- Control de acceso: este servicio proporciona protección contra el uso no autorizado de recursos accesibles mediante ISA. Estos recursos a los que se tiene acceso mediante protocolos de ISA, pueden ser o no de ISA. Este servicio de protección puede aplicarse a diversos tipos de acceso a un recurso (por ejemplo, el uso de un recurso de comunicaciones, la lectura, la escritura, o la supresión de un recurso de información; la ejecución de un recurso de procesamiento) o a todos los accesos a un recurso.
- Confidencialidad de los datos: estos servicios proporcionan la protección de los datos contra la revelación no autorizada.
    - Confidencialidad de los datos en modo sin conexión: este servicio proporciona la confidencialidad de todos los datos de usuario (N) en una unidad de datos de servicio (N) en modo sin conexión.
    - Confidencialidad de campos seleccionados: este servicio proporciona la confidencialidad de campos seleccionados en los datos de usuario (N) en el curso de una conexión (N) o en una unidad de datos de servicio (N) en modo sin conexión.

- Confidencialidad del flujo de tráfico: este servicio proporciona la protección de la información que pudiera derivarse de la observación de los flujos de tráfico.

- Integridad de los datos: estos servicios contrarrestan las amenazas activas.
- No repudio: puede adoptar una de las formas siguientes o ambas.
  - No repudio con prueba del origen: se proporciona al destinatario de los datos la prueba del origen de los datos. Esto lo protegerá contra cualquier tentativa del expedidor de negar que ha enviado los datos o su contenido.
  - No repudio con prueba de la entrega: se proporciona al expedidor de los datos la prueba de la entrega de los datos. Esto lo protegerá contra cualquier tentativa ulterior del destinatario de negar que ha recibido los datos o su contenido.

Mecanismos de seguridad específicos

Los siguientes mecanismos pueden incorporarse en la capa (N) apropiada para proporcionar algunos de los servicios descritos antes.

- Cifrado: el cifrado puede proporcionar la confidencialidad de la información o del flujo de tráfico.
- Mecanismos de firma digital: estos mecanismos definen dos procedimientos: firma de una unidad de datos; y verificación de una unidad de datos firmada.
- Mecanismos de control de acceso: pueden utilizar la identidad autenticada de una entidad o capacidades de la entidad, para determinar y aplicar los derechos de acceso de la entidad. Si la entidad intenta utilizar un recurso no autorizado, o un recurso autorizado con un tipo impropio de acceso, la función de control de acceso rechazará la tentativa y puede informar además el incidente para generar una alarma y/o anotarlo en el registro de auditoría de seguridad.
- Mecanismos de integridad de los datos: la integridad de los datos tiene dos aspectos: la integridad de una sola unidad de datos o de un solo campo, y la integridad de un tren de unidades de datos o de campos de unidad de datos. La determinación de la integridad de una sola unidad de datos

entraña dos procesos, uno en la entidad expedidora y otro en la entidad receptora. La entidad expedidora añade a una unidad de datos una cantidad que es en función de los propios datos. Esta cantidad puede ser una información suplementaria, tal como un código de control de bloque o un valor de control criptográfico, y puede estar cifrada. La entidad receptora genera una cantidad correspondiente y la compara con la cantidad recibida para determinar si los datos han sido modificados en tránsito.

Para la transferencia de datos en como con conexión, la protección de la integridad de una secuencia de unidades de datos requiere además alguna forma de ordenación explícita, como la numeración de secuencias.

- Mecanismo de intercambio de autentificación: se puede aplicar la utilización de información de autentificación, como contraseñas, suministradas por una unidad expedidora y verificadas, por la unidad receptora; técnicas criptográficas; y uso de características y/o propiedades de la entidad.

  Los mecanismos pueden incorporarse en la capa (N) para proporcionar autenticación de la entidad par.
- Mecanismo de relleno de tráfico: se utiliza para proporcionar diversos niveles de protección contra análisis de tráfico. Este mecanismo puede ser eficaz solamente si el relleno de tráfico está protegido por un servicio de confidencialidad.
- Mecanismo de control de encaminamiento: las rutas pueden elegirse dinámicamente o por acuerdo previo con el fin de utilizar solo subredes, relevadores o enlaces físicamente seguros. Al detectar ataques de manipulación persistentes, los sistemas extremos pueden dar instrucciones al proveedor del servicio de red que establezca una conexión por una ruta diferente.
- Mecanismo de notarización: pueden garantizarse las propiedades sobre los datos comunicados entre dos o más entidades, tales como su integridad, origen, fecha y destino, mediante la provisión de un mecanismo de notarización. La seguridad es proporcionada por una tercera parte que actúa como un notario, en el que las entidades comunicantes tienen

confianza y que mantiene la información necesaria para proporcionar la garantía requerida de una manera verificable.

La recomendación X.800 fue extraída de CCITT X.800 Redes de Comunicación de Datos: Interconexión de Sistemas Abiertos (ISA); Seguridad, Estructura y Aplicaciones. Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT, accedido el 30 de junio del 2014, https://www.itu.int/rec/T-REC-X.800-199103-I/es.

Para lograr proporcionar los servicios de seguridad que se indican en el marco del modelo de referencia de ISA, ayudándose con los mecanismo de seguridad citados anteriormente, para este trabajo se propuso la instalación y configuración de un firewall, el cual permitirá bloquear el acceso no autorizado permitiendo al mismo tiempo comunicaciones autorizadas.

1.3.5. Firewall

De acuerdo a la (Scarfone & Hoffman, 2009) NIST[29] Special Publication 800-41, Revision 1, los firewalls son dispositivos o programas que controlan el flujo de tráfico de red entre diferentes redes o hosts que emplean diferentes políticas de seguridad. Los firewalls generalmente trabajan en el contexto de la conectividad a internet, pero también pueden tener aplicabilidad en otros entornos de red. Por ejemplo, muchas redes empresariales emplean firewalls para restringir la conectividad hacia y desde las redes internas que brindan servicio a las funciones más sensibles de una empresa como la contabilidad, recursos humanos. Mediante el empleo del firewall se puede controlar el acceso a estas áreas y con esto una organización puede evitar el acceso no autorizado a sus sistemas y recursos.

Existen varios tipos de tecnologías de firewalls que están disponibles. Una forma de comparar sus capacidades es analizando que hace cada uno sobre las diferentes capas del Transmission Control Protocol/Internet Protocol (TCP/IP). Las comunicaciones con TCP/IP están compuestas de cuatro capas que funcionan en conjunto para transferir datos entre hosts. Cuando un usuario desea transferir datos, los datos se pasan de la capa más alta, a través de las capas intermedias a

[29] NIST: National Institute of Standars and Technology

la capa más baja, en cada capa se adiciona información, la capa más baja envía los datos acumulados a través de la red física, cuando los datos llegan a su destino pasan hacia la capa más alta desde la más baja, pasando por las intermedias. Las capas del protocolo TCP/IP se muestran en la Figura 1.6

Capa Aplicación: esta capa envía y recibe los datos de las aplicaciones particulares, como: Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), y Simple Mail Transfer Protocol (SMTP).
Capa Transporte: esta capa proporciona servicios con conexión o sin conexión para el transporte de los servicios de la capa aplicación entre las redes, y puede asegurar opcionalmente fiabilidad de las comunicaciones. Esta capa utiliza comúnmente loa protocolos Transmission Control Protocol (TCP) y User Datagram Protocol (UDP).
Capa Ip (Capa de red): esta capa rutea los paquetes a través de redes. Internet Protocol V.4 (IpV4) es el protocolo de capa de red fundamental para TPC/IP. Otros protocolos de uso son: IpV6, ICMP, and Internet Group Management Protocol (IGMP).
Capa Hardware (Capa física): esta capa se encarga de las comunicaciones en los componentes físicos de la red, el protocolo de esta capa es el Ethernet.

Figura 1.6 Capas TCP/IP, (Scarfone & Hoffman, 2009)

CAPÍTULO II

METODOLOGÍA

2. Metodología

2.1. Cómo diseñar un Data Center óptimo

Para el diseño del Data Center se ha tomado el estándar TIA-942 (TIA, 2005) como referencia, el cuál indica los requerimientos y directrices para el diseño e instalación de un Data Center, las consideraciones de diseño multidisciplinarias y los destinatarios.

2.1.1. Diseño Multidisciplinario

El estándar TIA-942 (TIA, 2005) tiene las siguientes consideraciones para el diseño multidisciplinario:

- Diseño arquitectónico (espacio, pisos, luz, seguridad, etc.)
- Cableado estructurado
- Sistema eléctrico
- Sistema de enfriamiento
- Operaciones

2.1.2. Áreas funcionales o espacios

El estándar TIA-942 (TIA, 2005), propone 5 áreas funcionales clave o para el diseño de un Data Center óptimo. Las cuáles son:

I. Uno o más cuartos de entrada (Entrance Room ER)
II. Área de distribución principal (Main Distribution Area MDA)
III. Área de distribución horizontal (Horizontal Distribution Area HDA)
IV. Área de distribución de zona (Zone Distribution Area ZDA), opcional.
V. Área de distribución de equipos (Equipment Distribution Area EDA)

Lo ideal sería que las áreas se encuentren en habitaciones separadas, pero esto no es práctico para las organizaciones normales; puede estar consolidado con áreas definidas. La distribución de los espacios se puede apreciar de mejor manera en la figura 2.1.

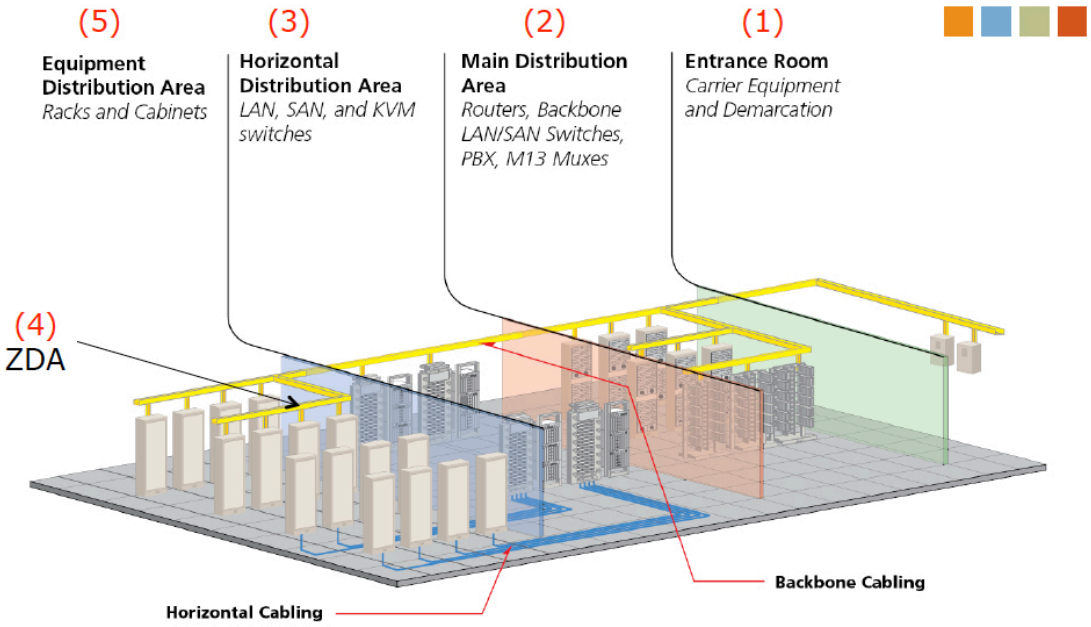


Figura 2.1. Espacios, ADC's Data Center Optical Distribution Frame: The Data Center's Main Cross-Connect

2.1.3. Diagrama de distribución

En un centro de datos bien diseñado las áreas funcionales deben garantizar que:

- Se pueda reasignar fácilmente el espacio, sobre todo en caso de crecimiento del Data Center.
- Se pueda operar fácilmente los cables, de manera que en el tendido de los mismos no se superen las distancias normadas.

En la figura 2.2 se puede observar un esquema de un Data Center que cumple con la TIA-942.

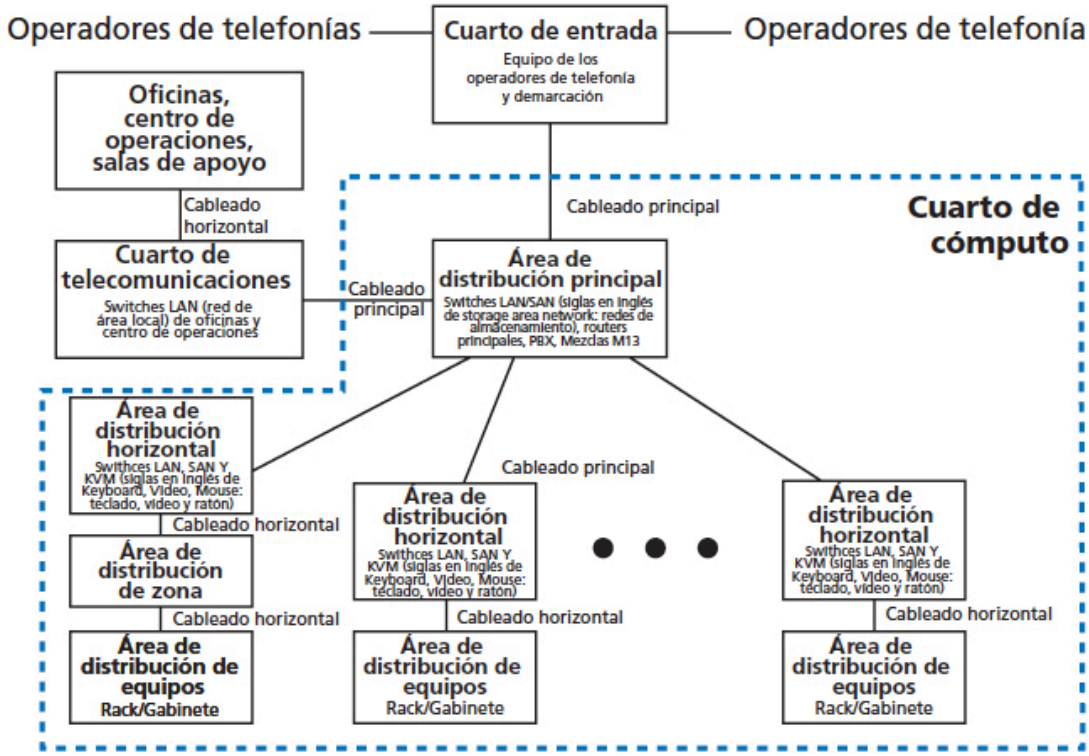


Figura 2.2 Data Center según TIA-942, (ADC, 2005)

2.1.4. Requerimientos de un Data Center

Los requerimientos típicos de un Data Center son:

Localización

- Evitar lugares que restrinjan expansión.
- Evitar el acceso redundante.
- Entrega de equipos grandes.
- Localizados lejos de fuentes EMI (Interferencia electromagnética).
- No debe existir ventanas al exterior (evitar el calor y riesgos de seguridad).
- Proporcionar acceso autorizado y monitoreado.

Tamaño

- Debe estar de acuerdo a los estándares que permiten cumplir con los requerimientos de las especificaciones de los equipos.
- Debe incluir un tamaño que permita el crecimiento de un futuro proyectado, así como las necesidades actuales.

Altura del techo

- Mínimo 259,08 cm desde el piso terminado hasta cualquier obstrucción (puede ser el techo, aspersores, accesorios de iluminación o cámaras).
- El sistema de refrigeración o enfriamiento puede necesitar techos más altos.
- Mínimo 45,72 cm de los sistemas rociadores de agua.

Pisos / Paredes

- Deben tener propiedades antiestáticas.
- Sellados para minimizar el polvo.
- Color de la luz, para mejorar la iluminación.

Puertas

- 91,44 cm de ancho X 213,36 cm de alto, no debe existir obstrucciones.

Iluminación

- Mínimo 500 lux[30] en plano horizontal y 200 lux en plano vertical.
- Iluminación separada sobre circuitos y paneles.
- Iluminación y señalización de emergencia.

Otros equipos

- UPS (Uninterruptible power supply).
- <= 100 kVa (Kilovoltios amperios) adentro de la habitación.
- > 100 kVa (Kilovoltios amperios) en habitación separada.

Parámetros operacionales

- Sistema dedicado HVAC (Heating, Ventilating, and Air Conditioning.)[31], preferiblemente (68 – 77 F), medido cada 304, 8 – 914,4 cm por la altura de 45,72 cm.
- HVAC – mínimo 100 sq ft/ton.
- Tasa máxima de cambio de temperatura: 5F/hr.

[30] Lux: es la unidad derivada del Sistema Internacional de Unidades para la iluminancia o nivel de iluminación. Equivale a un lumen /m².

[31] HVAC: Se le da este nombre al artefacto que puede controlar la calefacción, la ventilación y el aire acondicinado.

- 40 a 50 por ciento de humedad relativa (reduce la ESD Descarga electrostática)
- Los sistemas rociadores deben tener un mecanismo de acción previa.

Seguridad

- Cámaras de seguridad (internas y externas).

2.1.5. Mejores prácticas

- Localice el cuarto de entrada (ER) fuera del Data Center para fines de seguridad. Si está dentro del Data Center consolidar el cuarto de entrada (ER) con el área de distribución principal (MDA).
- El área de distribución principal (MDA) debe estar localizado en el centro.
- Tanto el área de distribución principal (MDA) y el área de distribución horizontal (HDA) requieren bastidores separados para los cables de fibra, UTP y coaxial.
- El área de distribución de zona (ZDA) es opcional, pero proporciona flexibilidad adicional.
- El área de distribución de equipos (EDA), contiene equipos solamente.
- Cada espacio requiere alimentación eléctrica y refrigeración.

2.1.6. Sistemas de cableado

La administración de los cables en un Data Center es permanente y genérica. Es como el sistema eléctrico, un servicio confiable y flexible al crecimiento al que se le puede conectar cualquier aplicación nueva.

Un sistema de cableado confiable de acuerdo con el estándar TIA-942 (TIA, 2005), debe cumplir los siguientes principios:

- Usar racks comunes en toda el área de distribución principal y las áreas de distribución horizontal.
- Instalar administradores de cables verticales y horizontales, comunes y extensos dentro y entre los racks.
- Instalar extensas trayectorias de cables para prever un crecimiento ordenado.

- Separar los cables UPT y coaxial de la fibra en el cableado horizontal, para evitar dañarla.
- El tendido de fibra se hace en un sistema de canales para evitar que se dañe.

Los sistemas de cableado se pueden apreciar de mejor manera en la figura 2.3.

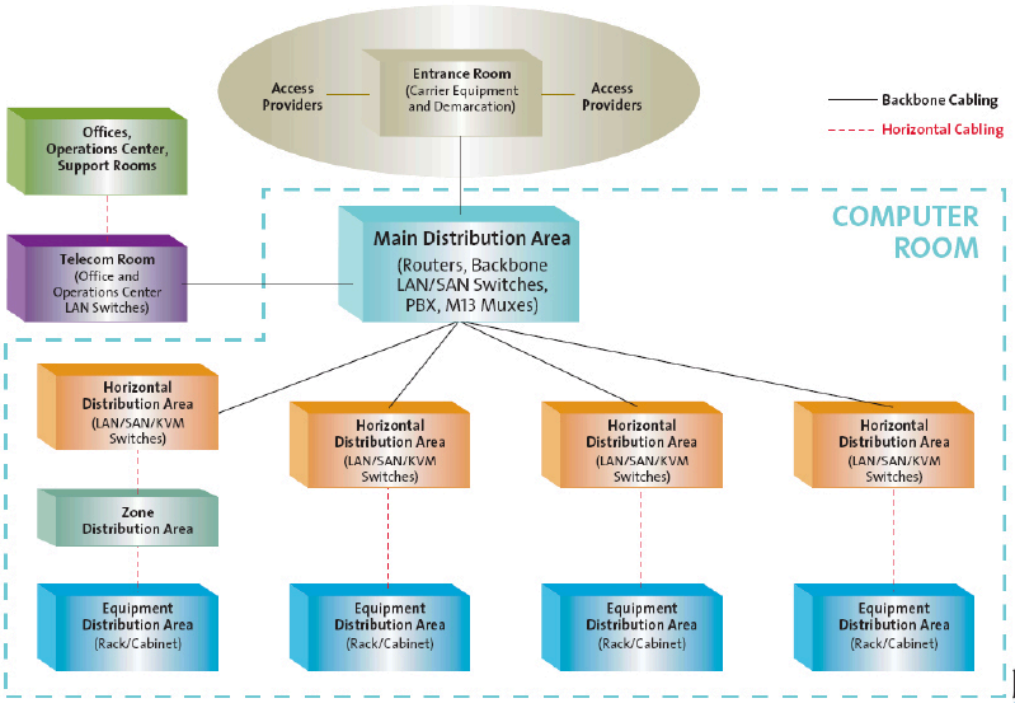


Figura 2.3. Sistemas de cableado, Corning Cable Systems – Just the Technical Facts

En la figura 2.3. se puede apreciar dos sistema de cableado: el cableado horizontal[32] (horizontal cabling) es el que une las áreas de distribución horizontal con las áreas de distribución de equipos y el cableado vertical[33] (backbone cabling) es el que une área de distribución principal con las áreas de distribución horizontal.

Una de las principales características de los sistemas de cableado es reducir la topología del Data Center, esto se logra consolidando el cuarto de entrada/área de distribución principal/área de distribución horizontal (ER/MDA/HAD), esto es

[32] Cableado horizontal: la norma EIA/TIA 568A lo define como la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones o viceversa.
[33] Cableado del backbone: proporciona interconexiones entre cuartos de entrada de servicios de edificio y cuartos de telecomunicaciones. Además incluye la conexión vertical entre pisos en edificios de varios pisos.

aplicable a la mayoría de las empresas. En la figura 2.4. se puede observar lo indicado.

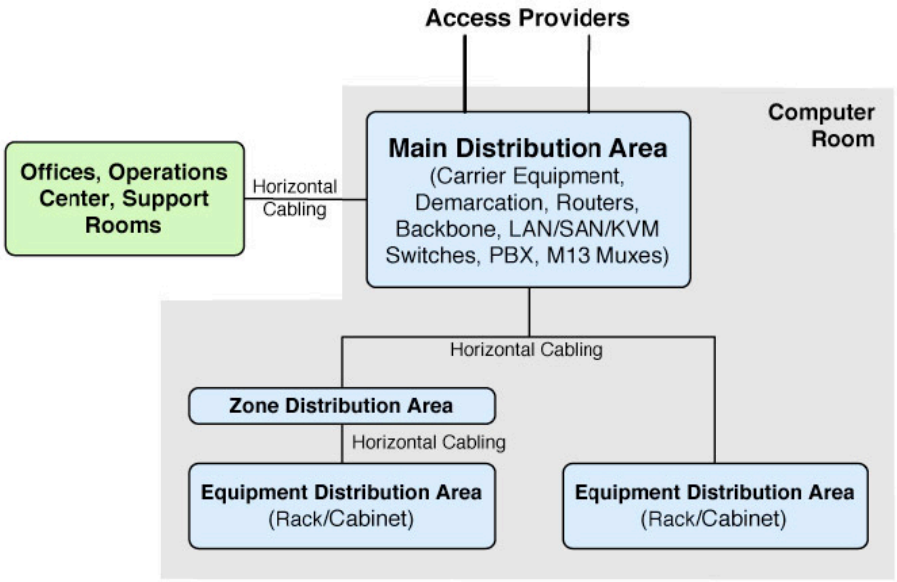


Figura 2.4. Consolidar ER/MDA/HAD, Orthronics – Standars-Based Data Center Structured Cabling System Design.

2.1.6.1. Medios de transmisión

- Cable de cobre – par trenzado 100 ohm.
  - Categoría 5e o 6, 6ª
  - 10GbE: categoría 6, 37-55 metros. Categoría 6A, 100 metros.
- Cable de fibra óptica multimodo
  - 62.5/125 µm o 50/125 µm.
  - 50/125 µm 850 nm láser optimizado mmf.
- Cable de fibra óptica monomodo.
- Cable coaxial 75 ohm.
  - Cable tipo 734 & 735
  - Conector coaxial tipo T1.404.

2.1.6.2. Racks y gabinetes

El manejo correcto de los cables, comienza en los racks y gabinetes, que deben ofrecer un amplio control sobre los sistemas de cableado horizontales y verticales. La función principal de los racks y gabinetes además de organizar los cables, es:

protegerlos, asegurar que no excedan los límites del radio de curvatura y manejar la holgura de los cables con eficacia (observar Figura 2.5).

Figura 2.5. Racks de cables, (ADC, 2005)

Para garantizar que los racks y gabinetes brinden una adecuada capacidad para manejar los cables, se realiza un cálculo a través de la fórmula siguiente (este cálculo es aplicable para UTP categoría 6):

Fórmula: cables X 0.0625 pulgadas cuadradas (diámetro del cable) X 1.30 = necesidad de manejo del cable.

Se multiplica por 1.30 para garantizar que no supere el 70% de capacidad.

Ejemplo: 350 cables X 0.0625 X 1.30 = 28.44 pulgadas cuadradas (Racks o gabinetes mínimo 6 pulgadas X 6 pulgadas o 4 pulgadas X 8 pulgadas).

2.1.7. Consideraciones eléctricas

Las consideraciones eléctricas son la parte vital del centro de datos. Un corte de energía de apenas segundos podría ocasionar daños en los servidores. Para garantizar un suministro de energía confiable las buenas prácticas incluyen:

- Múltiples conexiones de red eléctrica.
- Breakers por cada rack o circuitos.

- Configuración de UPS (Suministro de alimentación ininterrumpible / Uninterrupted power supplies)
- Circuitos múltiples.
- Generadores en-sitio.
- Capacidad del generador para incluir el sistema de enfriamiento.
- Capacidad del UPS para incluir el sistema de enfriamiento y las luces.
- Tomar en cuenta el crecimiento.

2.1.8. Consideraciones del sistema de enfriamiento

Implicaciones del diseño para sacar el calor de los Data Centers:

- Tener equipos de refrigeración adecuados.
- Circulación del aire.
- Usar el procedimiento “hot aisle / cold aisle” (pasillo caliento/pasillo frío), es una configuración donde los racks de los equipos se colocan el filas alternas de pasillos calientes y fríos. En el pasillo frío los racks de los equipos se disponen frente e frente. En el pasillo caliente, están la parte posterior con la parte posterior (ver Figura 2.6). las placas perforadas en el piso elevado de los pasillos fríos permiten que llegue aire frío al frente de los equipos. Este aire frío envuelve al equipo y se expulsa por la parte trasera hacia el pasillo caliente (ADC, 2005).
- Diseño de racks y gabinetes en filas.
- Localización de las unidades de climatización CRAC.
- Cantidad y ubicación de ventoleras.
- Dimensionamiento de conductos.
- Configuración interna adecuada de los racks.
-

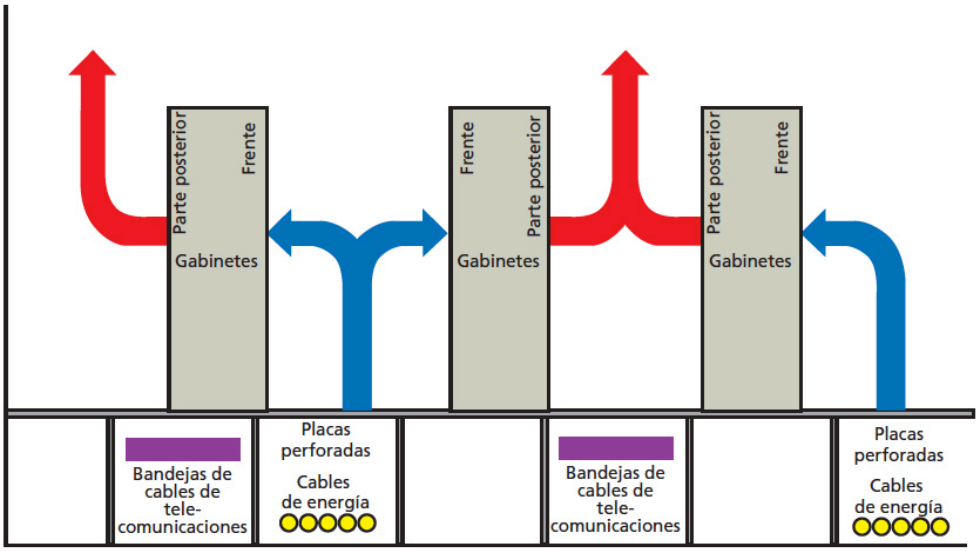


Figura 2.6. Pasillos calientes y pasillos fríos, (ADC, 2005)

2.2. Análisis comparativo entre sistemas de virtualización

Para el desarrollo de este trabajo, en el Capítulo I se realizó un estudio teórico acerca de las principales características de cada una de las plataformas para infraestructuras virtuales: Microsoft Windows 2012 Server Hyper-V y VMware vSphere ESXi 5.5. Teniendo como resultado:

Ventajas clave de VMWare vShpere

- **Eficiencia mediante utilización y automatización:** se puede lograr índices de consolidación con una relación de 15:1 o más y mejora la utilización de hardware del 5% al 80% o más sin sacrificar el rendimiento.
- **Disminución considerable de los costos de TI:** se logra una reducción de entre el 20%y el 30% en costos de infraestructura de TI por cada aplicación
- **Agilidad con control:** ayuda a responder rápidamente a nuevos requerimientos del negocio sin sacrificar seguridad y control. Además suministra una infraestructura sin intervenciones, con garantías de disponibilidad, escalabilidad y rendimiento para todas las aplicaciones críticas del negocio que se ejecuten en vSphere.
- **Libertad de elección:** utilice una plataforma común basada en estándares para aprovechar los activos de TI que ya posee.

Texto tomado de: VMWare, 2014. Hoja de Datos VMWare vSphere – La plataforma de virtualización líder del mundo,

http://www.vmware.com/files/latam/pdf/products/vsphere/VMware-vSphere-Datasheet.pdf, accedido el 8 de septiembre de 2014.

Ventajas clave de Windows Server 2012 Hyper-V

- **Live Migration:** se puede mover máquinas virtuales de un nodo a otro nodo sin interrupción.
- **Cluster Shared Volumes:** se garantiza alta disponibilidad y uso flexible de almacenamiento compartido (SAN) para almacenar máquinas virtuales.
- **Processor Compatibility:** aumenta la flexibilidad de Live Migration entre hosts con distinta arquitectura.
- **Hot Add Storage:** se puede añadir o eliminar almacenamiento a las máquinas virtuales en caliente.
- **Dynamic Memory:** uso eficiente de la memoria, permitiendo mantener el rendimiento consistente en la máquina virtual.
- **Virtual Fiber Channel:** se puede integrar directamente la máquina virtual con la SAN.
- **New Virtual Hard Disk Format (VHDX):** nuevo formato de máquinas virtuales, permite escalar hasta 64TB de tamaño.
- **Resource Metering:** analiza el tráfico IP de una dirección o máquina virtual para asegurar que la carga de trabajo sea correcta.
- **Data Center Bridging (DCB):** nuestra LAN a 10 GB**.**

Además se pudo determinar los atributos para la implementación de VMWare y Microsoft Windows, los cuáles se pueden observar en la siguiente tabla:

Atributos de Hypervisor	**VMware vSphere 5.5**	**Windows Server 2012 with Hyper-V**
Huella en disco	<200MB	>5GB con instalación de núcleo servidor Alrededor de 10Gb en instalación completa
Independencia de SO	No depende del sistema operativo en propósito general	Se basa en Windows server 2012 en la partición principal

Atributos de Hypervisor	**VMware vSphere 5.5**	**Windows Server 2012 with Hyper-V**
Hardened Drivers	Optimización para distribuidores de hardware	Drivers Genéricos de Windows
Manejo de memoria avanzada	Capacidad para recuperar la memoria no utilizada, páginas de duplicado de memoria, comprimir las páginas de memoria, swap de disco / SSD	Sólo utiliza ballooning, requiere drivers especiales-no Linux, no NUMA
Manejo de CPU avanzado	Ajustado para apoyar Intel SMT hyper-threading; Soporta aceleradores de gráficos 3D	Ninguna ventaja de rendimiento fiable al utilizar Hyper-Threading
Administración de almacenamiento avanzada	vSphere Sistema de archivos de la máquina virtual	Carece de un sistema de archivos en clúster integrado
Tecnología de seguridad virtual	vCloud Networking y Seguridad, Activa el nivel de seguridad de introspección del hypervisor	Mínima adopción de su estándar de seguridad. Plug-ins de terceros necesarios
Asignación de Recursos Flexible	Hot add de VM vCPUs y memoria, aumento de volumen VMFS, extensión en caliente de discos virtuales, añadido en caliente de los discos virtuales	Nada comparable
Patching Simplificado	Patching sin relación; El Patching basado en imagenes con capacidades de rollback proporciona parches limpios y sencillos	Sujeto a frecuente patching relacionado con el S.O; La compleja arquitectura del patching requiere esfuerzo y complejidad adicional

Tabla 2.1. Tabla comparativa de los atributos de Exsi 5.5 y Hyper-V, (Nicolalde, 2014)

Como se puede observar en la tabla anterior una de las principales ventajas de VMWare Esxi 5.5 es que utiliza menos de 200 MB de espacio en disco para su instalación, permitiendo que casi todo el espacio del disco quede disponible para

las virtuales. Además no corre sobre ningún sistema operativo, disminuyendo la huella del hardware de servidor, el consumo de energía y el costo.

Como conclusión luego de analizar las características de Esxi 5.5 y Hyper-V, se ha llegado a determinar que la opción que se adapta mejor a las necesidades del Museo QCAZ es la presentada por VMWare Esxi 5.5. Por la manera eficiente con la que administra el hardware del servidor, primeramente permite disponer de mayores recursos para las máquinas virtuales y además se puede utilizar hardware de generaciones anteriores (en nuestro caso estamos implementando la infraestructura virtual sobre un servidor Hp Proliant DL385G6 con 2 procesadores de 6 núcleos cada uno, 32 GB de memoria RAM y 8TB de almacenamiento).

2.3. Diagnóstico del tráfico de la red del Museo QCAZ con Wireshark

El objetivo del presente diagnóstico es determinar el tráfico entrante y saliente que hay en la red del Museo QCAZ, y en base a este análisis, fijar el mejor mecanismo que se puede emplear para mantener la información segura de cualquier ataque interno o externo y además que no exista pérdida del rendimiento de la red.

Con el analizador de tráfico WireShark (open-source), se puede detectar, analizar y correlacionar el tráfico en tiempo real identificando las amenazas de red, para posteriormente limitar su impacto.

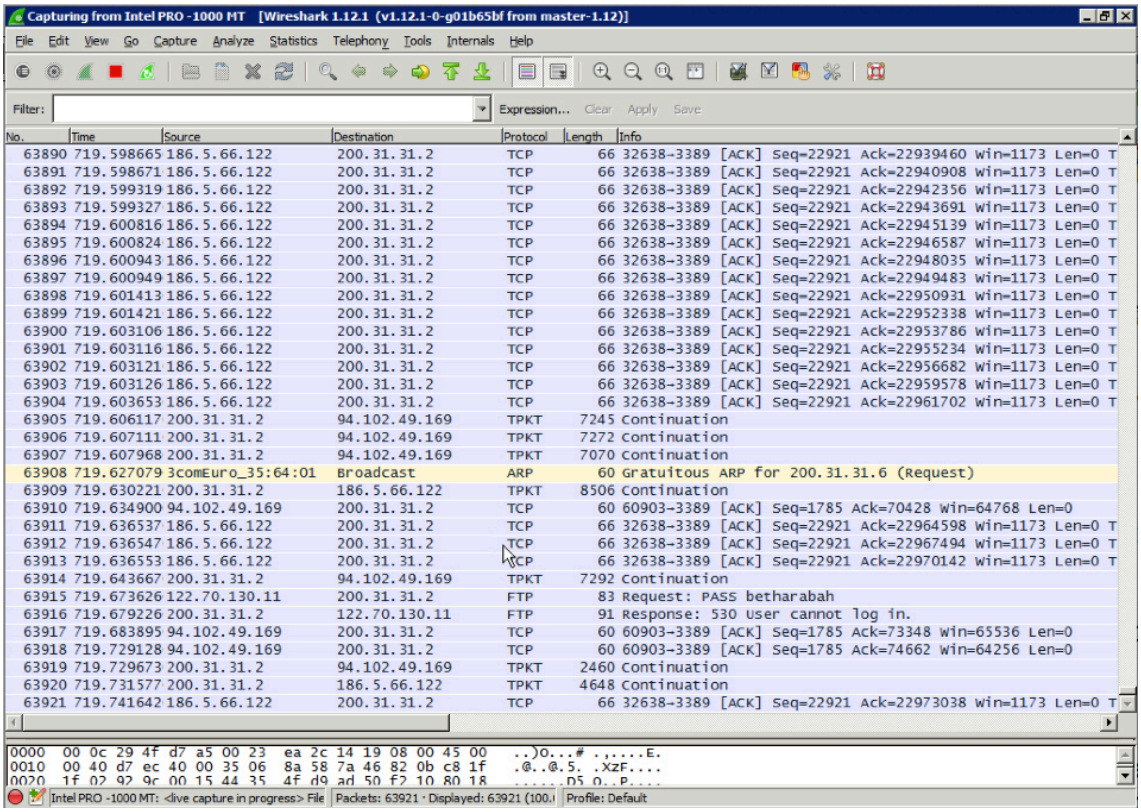


Figura 2.7. Captura de la monitorización del tráfico del servidor web del QCAZ, (Nicolalde, 2014)

2.3.1. Tipos de ataques a analizar

ARP SPOOF[34].

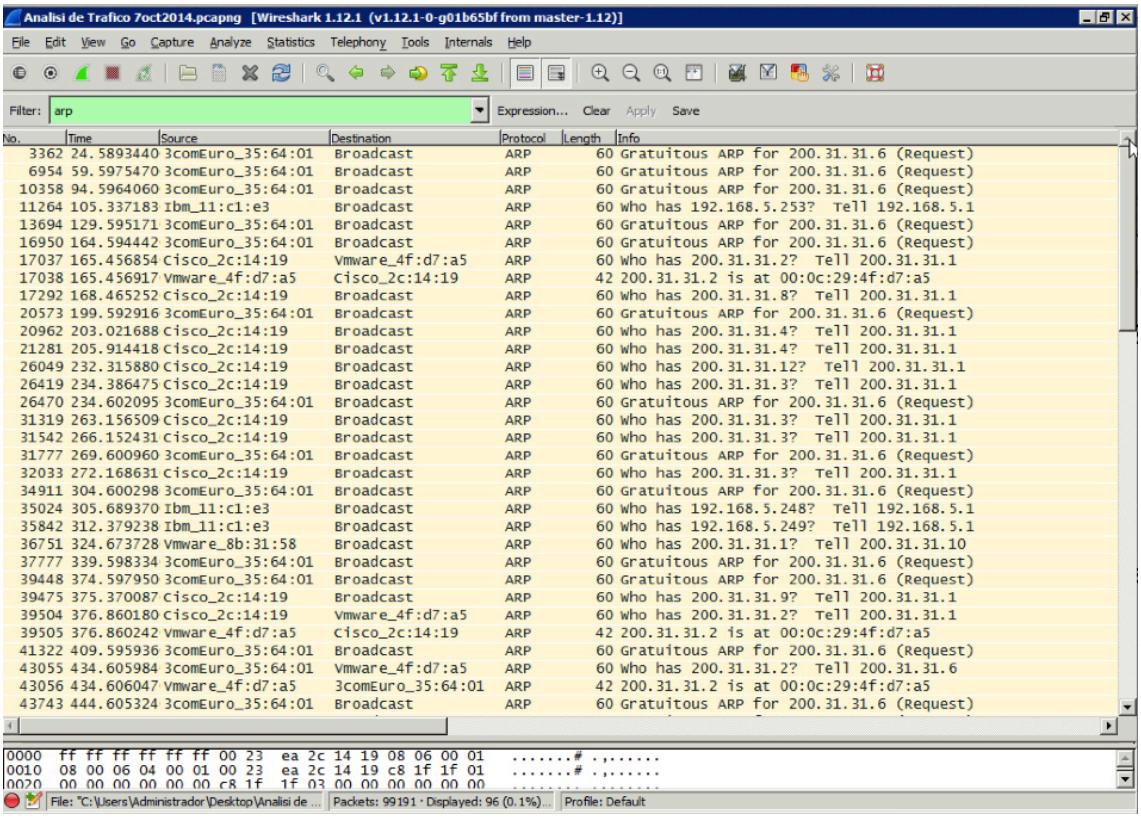


Figura 2.8. Comportamiento del protocolo ARP en el QCAZ, (Nicolalde, 2014)

Observando detenidamente el tráfico de la red en la figura 2.8, se puede deducir que no está ocurriendo nada sospechoso que permita pensar que se está siendo víctima de una ataque Arp Spoof, ya que no se puede observar paquetes ARP reply falsos, es decir, no existen paquetes que tengan diferentes ip con una misma dirección MAC.

Para mitigar este tipo de ataques se recomiendo monitorear el tráfico de la red de manera permanente e instalar alguna herramienta (Arpwatch, Nast, Snort, Patriot NG, ArpON) que permita alertar al administrador de la red cuando se detecte el uso anormal del protocolo ARP.

[34] ARP SPOOF: es una técnica usada para infiltrarse en una red Ethernet conmutada (basada en *switches*), que puede permitir al atacante leer paquetes de datos en la LAN, modificar el tráfico, o incluso detenerlo.

Port Flooding[35]

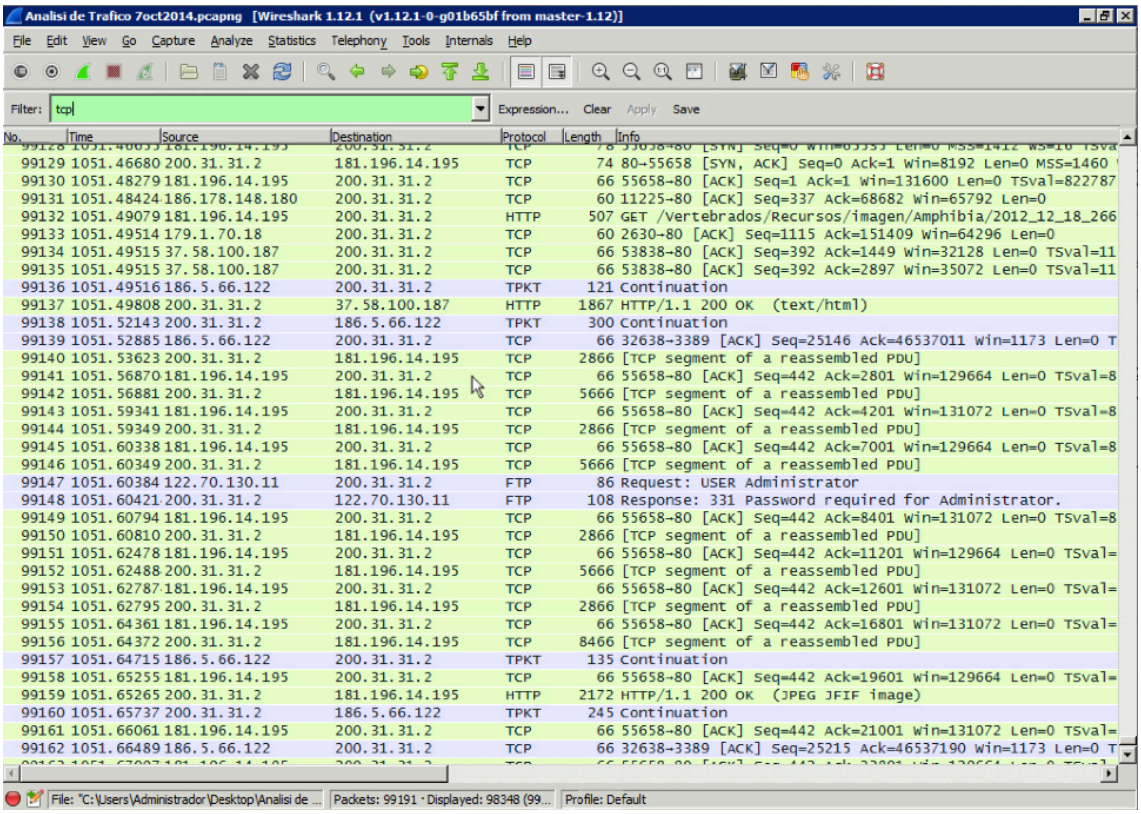


Figura 2.9. Comportamiento del protocolo TCP del QCAZ, (Nicolalde, 2014)

Observando el comportamiento del protocolo TCP en la figura 2.9. se puede observar que no se está recibiendo tramas no legítimas, ya que ninguna trama presenta una ip diferente con la misma MAC.

Para mitigar este tipo de ataques se debe instalar en la red un analizador de protocolos, ya que mirando el tráfico generado se nota la existencia de una gran cantidad de tramas con valores aleatorios o no.

[35] Port Flooding: consiste en enviar múltiples tramas falsificadas a través de un puerto con el objetivo de llenar la tabla de asignación del *switch*. Un switch dispone de una memoria interna CAM (Content-Addressable Memory) donde asigna puertos a direcciones MAC.

DDOS ATTACKS[36]

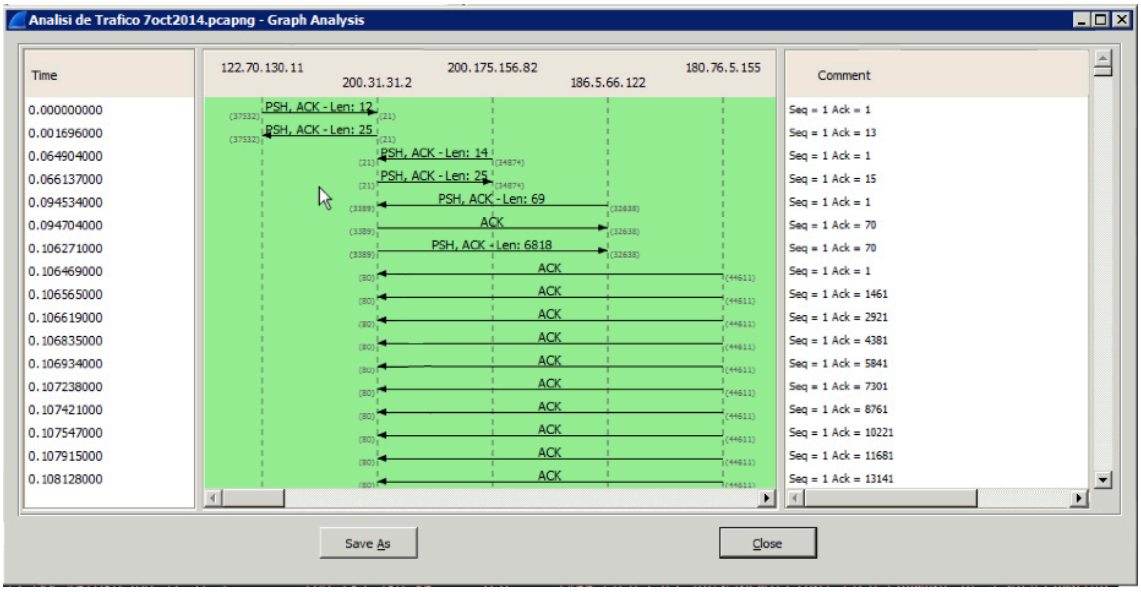


Figura 2.10. Gráfico de flujo, (Nicolalde, 2014)

En la figura 2.10 no se observa que exista una gran cantidad de segmentos TCP con el flag SYN activados desde una misma ip en un intervalo muy corto de tiempo. Por lo que se puede descartar que exista un ataque de denegación de servicio en la red del QCAZ.

Cuando existe un gran volumen de tráfico en la red, frenar este tipo de ataques es bastante complicado, una forma de mitigarlo es comprando equipos propios para el efecto, aunque esta solución resulta muy costosa para las organizaciones, por esto la mejor opción es contactarle directamente al proveedor. Sin embargo, cuando el ataque DDoS no es extremado, una buena solución consiste en una configuración adecuada del sistema operativo y de los servicios afectados.

DHCP SPOOF[37]

Este tipo de ataque no aplica para la red del Museo QCAZ, ya que no existe un servidor DCHP para el direccionamiento dinámico de la red.

[36] DDoS ATTACKS: ataques de denegación de servicio (DoS)
[37] DHCP SPOOF: consiste en falsificar paquetes DHCP

En la siguiente imagen podemos observar que no existe un uso anormal del protocolo DHCP y además no hay errores en las máquinas de la red indicando Ips duplicadas.

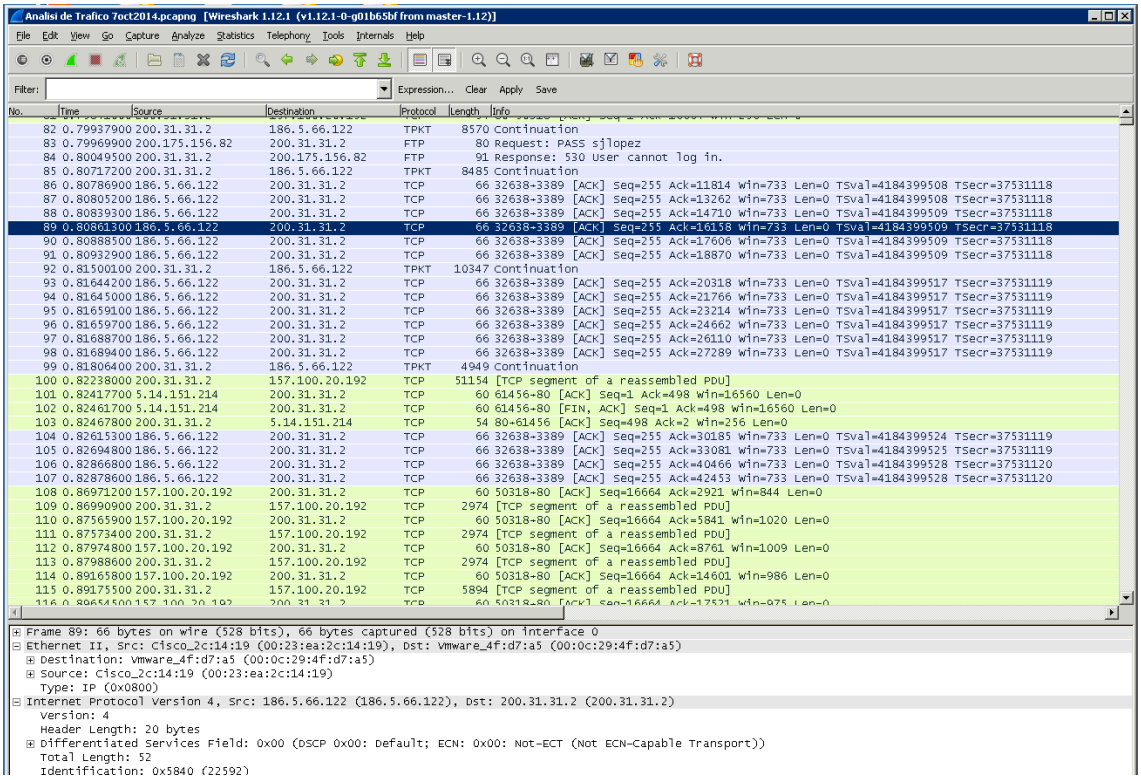


Figura 2.11. Paquetes capturados con Wireshark, (Nicolalde, 2014)

“El protocolo DCHP no proporciona mecanismos de autenticación que permitan verificar el origen de los paquetes durante la negociación entre el servidor y el cliente, por lo que cualquier atacante puede falsificar los paquetes DHCPOFFER proporcionado información falsa al cliente.

Un escenario de ataque podría proporcionar como puerta de enlace la propia Ip del atacante con el fin de recibir paquetes destinados hacia fuera de la LAN. El atacante podría enrutar esos paquetes hacia el sitio legitimo con el objetivo de hacer el ataque totalmente transparente para el usuario.”[38]

La mejor forma de mitigar este tipo de ataque es instalando herramientas que alerten sobre estas situaciones. Con Wireshark por ejemplo, se pueden usar filtros para acelerar la búsqueda de respuestas ACK con un DNS o una puerta de enlace diferentes, al configurado en nuestro servidor DHCP.

[38] Tomado de: (Febrero, 2011)

VLAN HOPPING

Se presenta cuando existe un ataque a una red que tiene configurada dentro de su estructura VLAN's, el método analizado fue el de suplantación del switch.

- **Ataque de suplantación de switch**

Para que este ataque funcione, el equipo atacante debe estar configurado de tal manera que sea capaz de manejar los protocolos de etiquetado (ISL) y concentración de enlaces (DTP[39]) utilizados entre switches de la red, imitando el comportamiento de un switch más de la red. De esta forma se lograría acceso al resto de tráfico de la red ya que el equipo se volvería miembro de todas las VLAN[40], siempre y cuando el o los puertos del switch estén configurados como dynamic auto[41] o desirable[42].

En la figura 2.12 se puede observar que no existe un comportamiento anormal del protocolo DTP, por lo que se puede descartar que la red del museo QCAZ esté sufriendo este tipo de ataques.

Para mitigar este tipo de ataques hay que configurar los puertos expuestos a usuarios como access port o configurar el estado DTP como no negociable, para que se ignoren las negociaciones trunk.

[39] DTP: Dynamic Trunk Protocol
[40] Tomado de (Febrero, 2011)
[41] Cuando uno o varios puertos del switch están en modo dynamic auto, simplemente escucha tramas DTP provenientes de switches vecinos que tengan la intención de crear un enlace trunk.
[42] Cuando uno o varios puertos del switch están en modo dynamic desirable, es el propio puerto el interesado en crear un enlace trunk mediante el envío de tramas de negociación DTP a los switches vecinos.

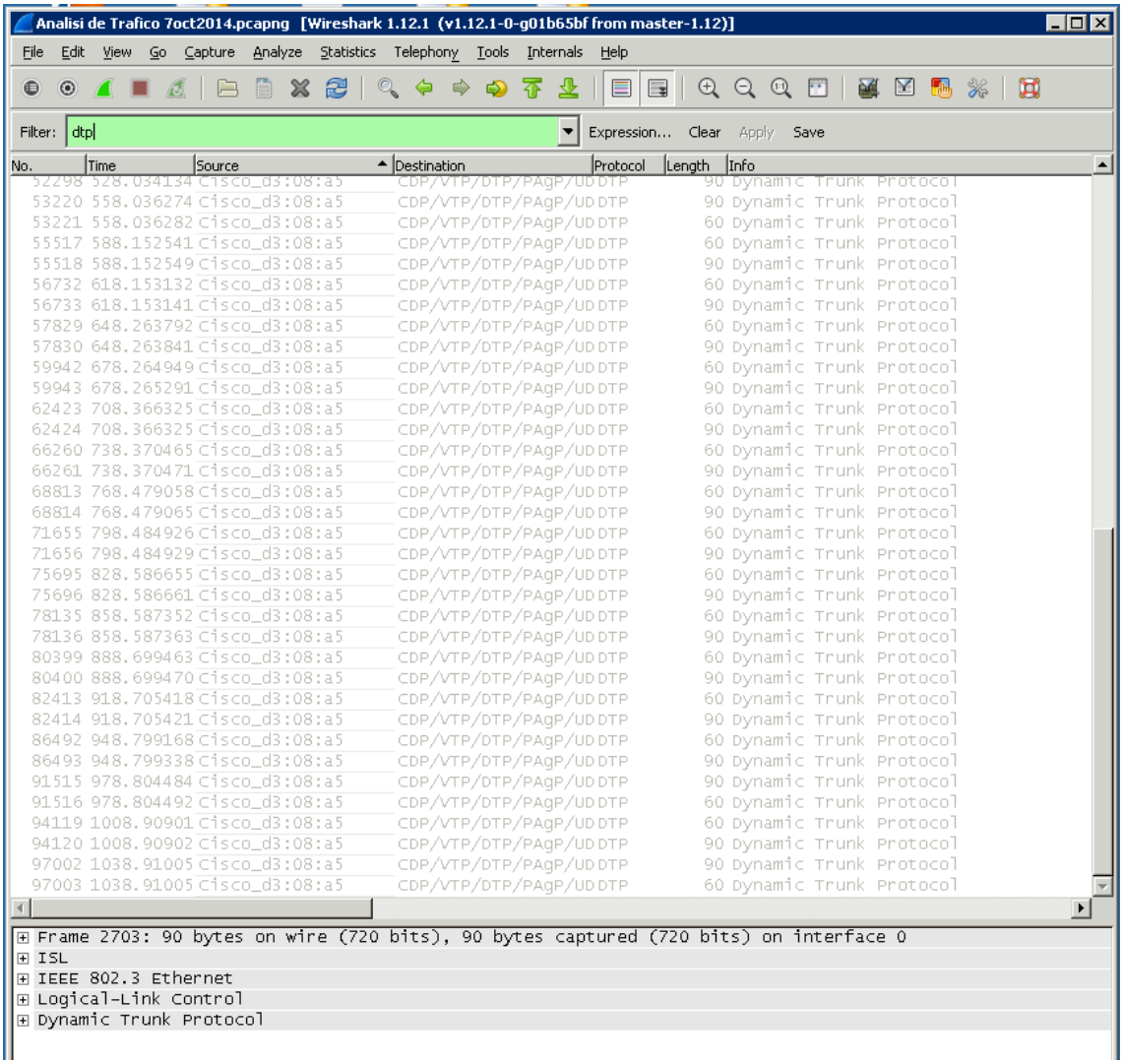


Figura 2.12. Protocolo DTP, (Nicolalde, 2014)

2.3.2. Análisis de MALWARE

La cantidad de malware es infinita y está en constante evolución. A pesar de los esfuerzos de las empresas de antivirus por desarrollar programas efectivos, siempre están un paso por detrás, por lo que siempre se dan casos de programas maliciosos que alcanzan al equipo del usuario.

En la figura 2.13 se puede identificar el software que se ha descargado desde el servidor de todas las peticiones http detectadas en la captura del tráfico. Como se puede observar todas las peticiones http vienen del servidor del Museo QCAZ, por tal motivo se puede descartar la existencia de Malware en el tráfico analizado.

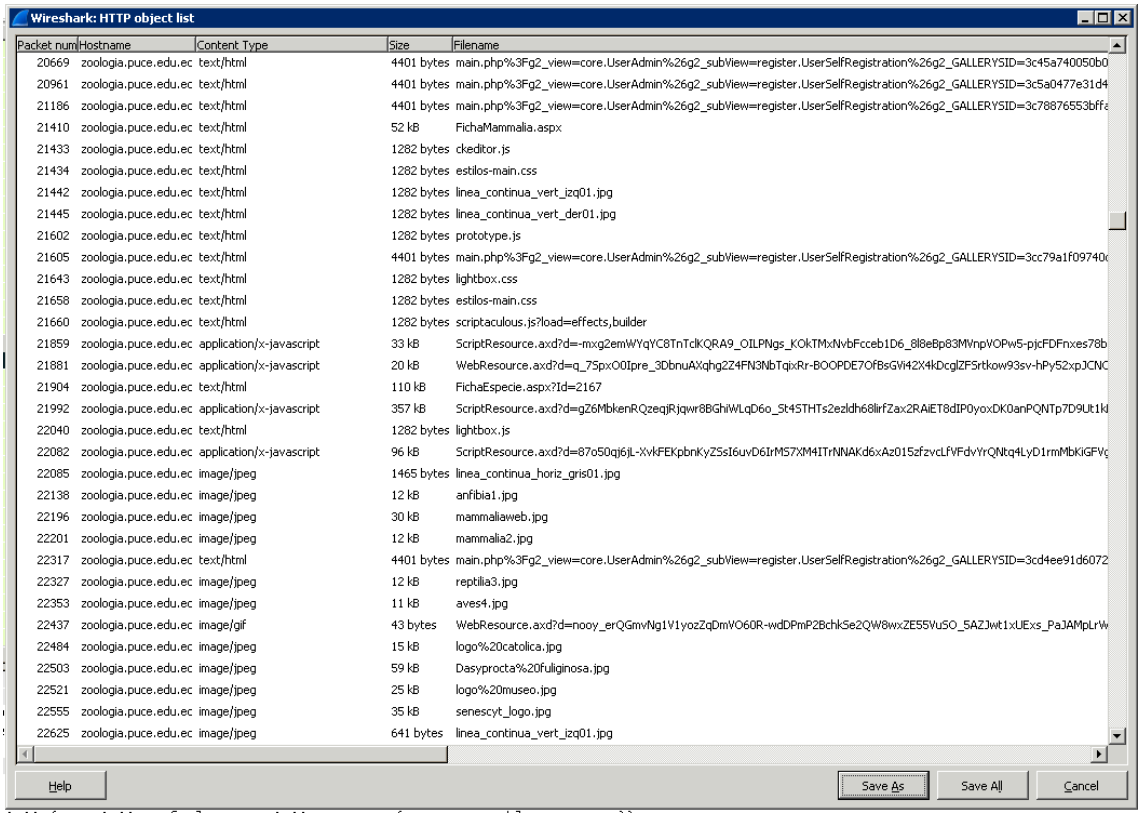


Figura 2.13. Lista de objetos http, (Nicolalde, 2014)

La única forma de mitigar este tipo de ataques (aunque no se puede mitigar al 100%) es manteniendo todos los sistemas y aplicaciones actualizadas y concientizando a los usuarios de la red el peligro de infección cuando se descarga software de sitios desconocidos.

2.3.3. Filtros

Cuando se tienen un gran volumen de tráfico en la red, es difícil hacer un análisis del mismo, con Wireshark se facilita el trabajo gracias a que esta herramienta presenta un opción que permite filtrar el tráfico y mostrar únicamente aquellos paquetes que están de acuerdo al criterio de búsqueda, facilitando enormemente el análisis del tráfico de la red.

Con Wireshark se puede filtrar el tráfico a través de filtros de captura y filtros de visualización. Los filtros de captura funcionan con las librerías libpcap[43], por lo que dependen de las mismas par definir los filtros. Los filtros de visualización siguen

[43] Libpcap: es una librería de funciones, cuyos procesos se realizan a nivel de usuario, además las capturas de los paquetes del tráfico de la red se realiza a nivel de kernel, esta librería gestiona la captura medinte los filtros establecidos.

una nomenclatura propia de la aplicación y se emplean para obtener resultados en base a paquetes previamente capturados.

Para el caso del Museo QCAZ primero se empleo un filtro de retransmisiones para filtrar los paquetes duplicados y de esta manera eliminar el ruido de la captura. En la figura 2.14 se puede observar los paquetes ya filtrados.

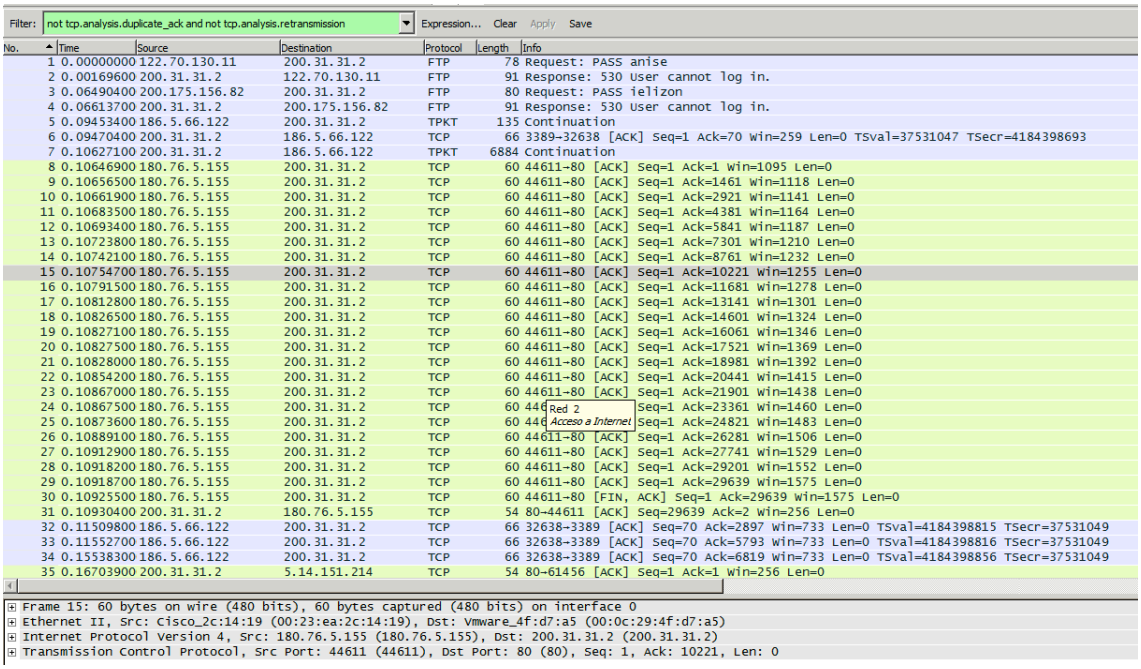


Figura 2.14. Paquetes después de usar el filtro de retransmisiones,(Nicolalde, 2014)

También se utilizó el filtro de cookies (http.cookie and http.host contains “facebook”), con la finalidad de capturar sesiones por ejemplo de facebook cuyas cookies viajen por la red, se llego a la conclusión que la red esta con un tráfico normal.

2.3.4. Análisis Follow TCP stream

Con esta opción se puede extraer el flujo de datos establecido en una sesión TCP, en la figura 2.15 se puede observar que esta funcionalidad no se limita a un análisis superficial.

Se realiza una petición desde un host remoto hacia el servidor zoología.puce.edu.ec para que este despliegue una fotografía en formato jpg, se puede observar la fecha de modificación, el servidor desde donde se despliega, en este caso es un Internet Information Server IIS versión 7.5, el tamaño del

contenido, etc., si se quisiera llevar a cabo in análisis más detallado y conocer las intenciones del atacante se podría traducir el código con cualquier desensamblador.

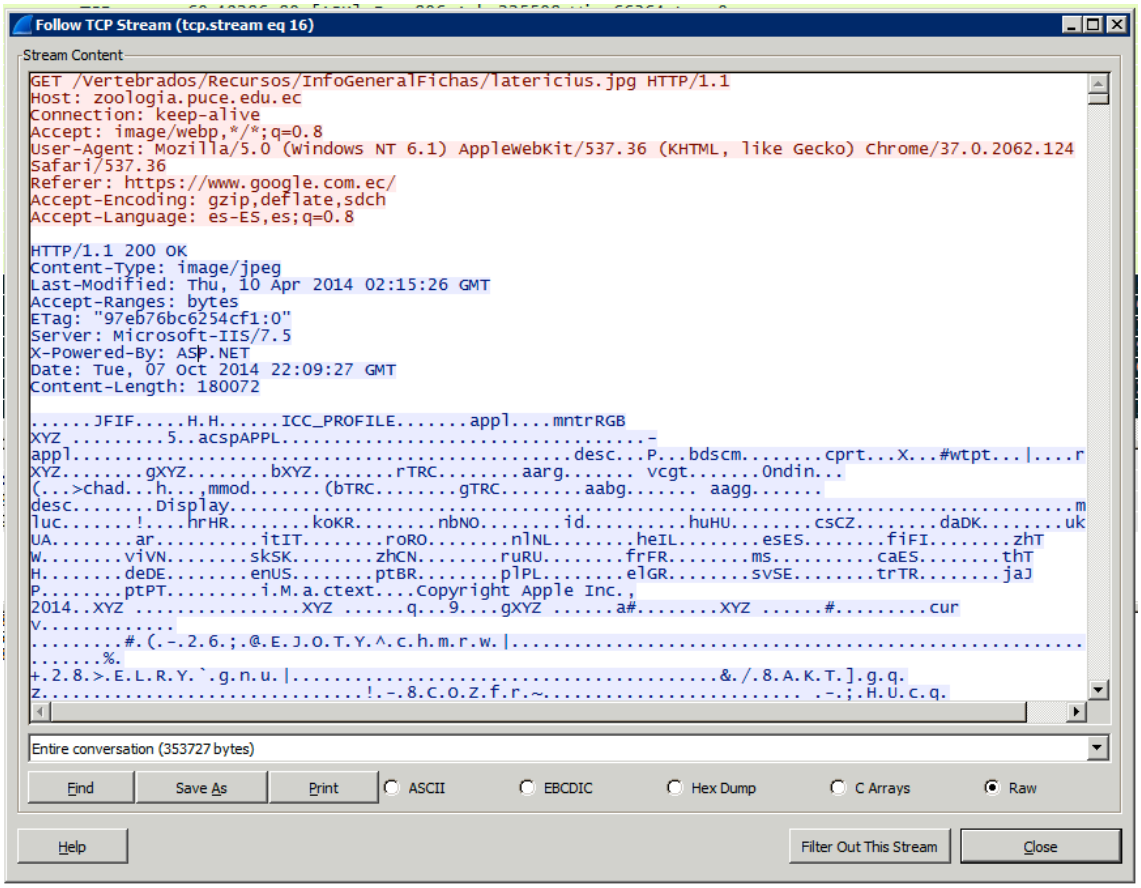


Figura 2.15. Follow TCP Stream, (Nicolalde, 2014)

Expert infos

Wireshark trae consigo una herramienta muy útil llamada Experts Infos, con esta se puede analizar el tráfico de manera muy detallada, cada entrada de análisis contiene la siguiente información: criticidad, grupo, protocolo y resumen. Es un archivo de registro de las anomalías encontradas por Wireshark en una captura de tráfico, los niveles usados son:

Severity[44]

Chat (aparecen en color gris): cuando la información sobre el flujo es normal.

[44] Tomado de: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html, accedido el 27 de octubre de 2014

Nota (aparecen en color cian): cuando la información sobre el flujo no es normal.

Advertencia (aparecen en color amarillo): indican que la información sobre el flujo necesita atención.

Error (aparecen en color rojo): indican problemas graves, coma paquetes mal formados.

Group[45]

Checksum: una suma de comprobación no es válida.

Secuencia: secuencias de protocolo sospechosas.

Código de Respuesta: problemas con códigos de respuesta de aplicaciones.

Código de petición: una petición a una aplicación.

Sin decodificar: disección incompleta o los datos no se pueden decodificar por otros motivos.

Ensamblado: problemas en el reensamblado. Por ejemplo, no se cuenta con todos los fragmentos u ocurrió una excepción durante el proceso.

Protocolo: violación de las especificaciones del protocolo como, por ejemplo, los valores de campo son inválidos o las longitudes ilegales.

Mal formados: paquetes mal formados o en el análisis se produjo un error que produjo que se abortara el análisis.

Con este antecedente en la figura 2.16 se puede observar el Export Infos del flujo del tráfico de la red del Museo QCAZ.

[45] Tomado de: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html, accedido el 27 de octubre de 2014

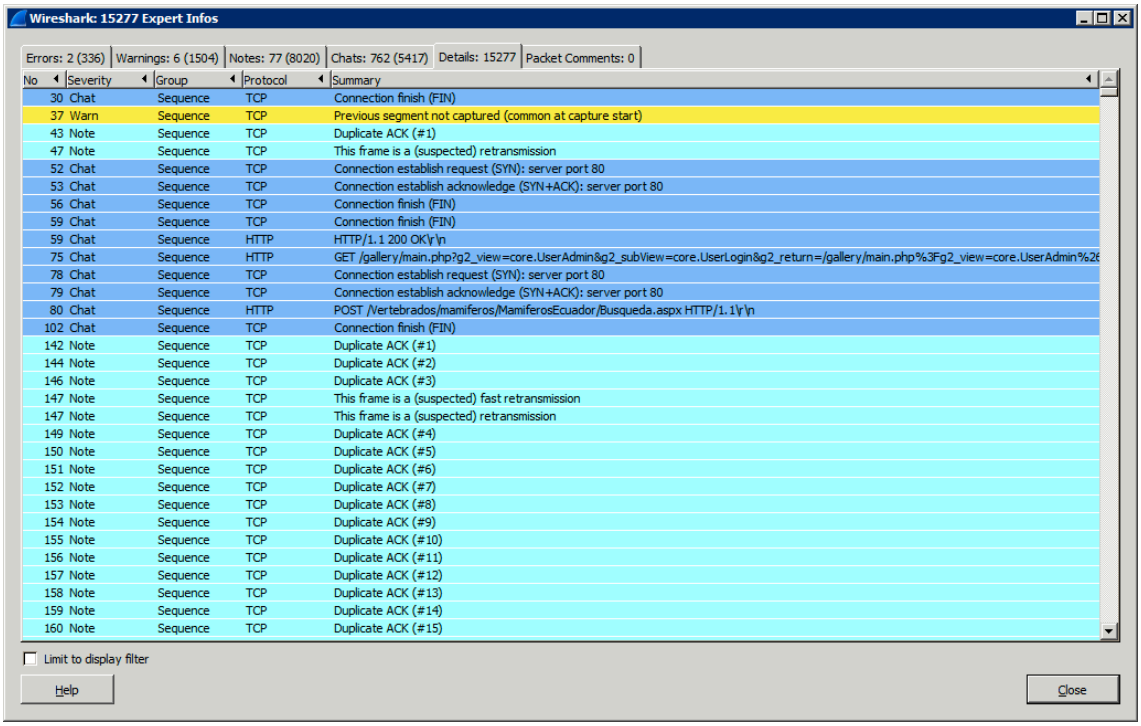


Figura 2.16. Export Infos del flujo el tráfico del Museo QCAZ, (Nicolalde, 2014)

Como se puede observar en la figura anterior, tenemos un flujo aparentemente normal, de todas maneras el paquete 37 necesita atención ya que podría ser intento de ataque.

2.3.5. Gráficos de Wireshark

Cuando hay que evaluar los paquetes que circulan por la red, Wireshark proporciona una variedad de opciones para hacerlo de forma gráfica. Se puede dar seguimiento a una traza TCP de forma gráfica de manera que se visualice la relación existente de tiempo/número de secuencia en un flujo de datos, esta gráfica se llama Time Secuencie Graph (Steven).

Observando la figura 2.17 se puede interpretar que la conexión de la red del Museo QCAZ esta dentro de los parámetros para ser considerada como ideal, se puede observar claramente una línea creciente con el tiempo en forma de pendiente, lo que muestra un rendimiento eficiente de la conexión TCP. Sin embargo también se puede observar huecos que interrumpen la continuidad de la línea lo que indica que existen segmentos perdidos, ack duplicados, timeout

vencidos[46], etc.. En el caso del Museo QCAZ estos huecos se deben a que existen muchos segmentos TPC reensamblados de una PDU.

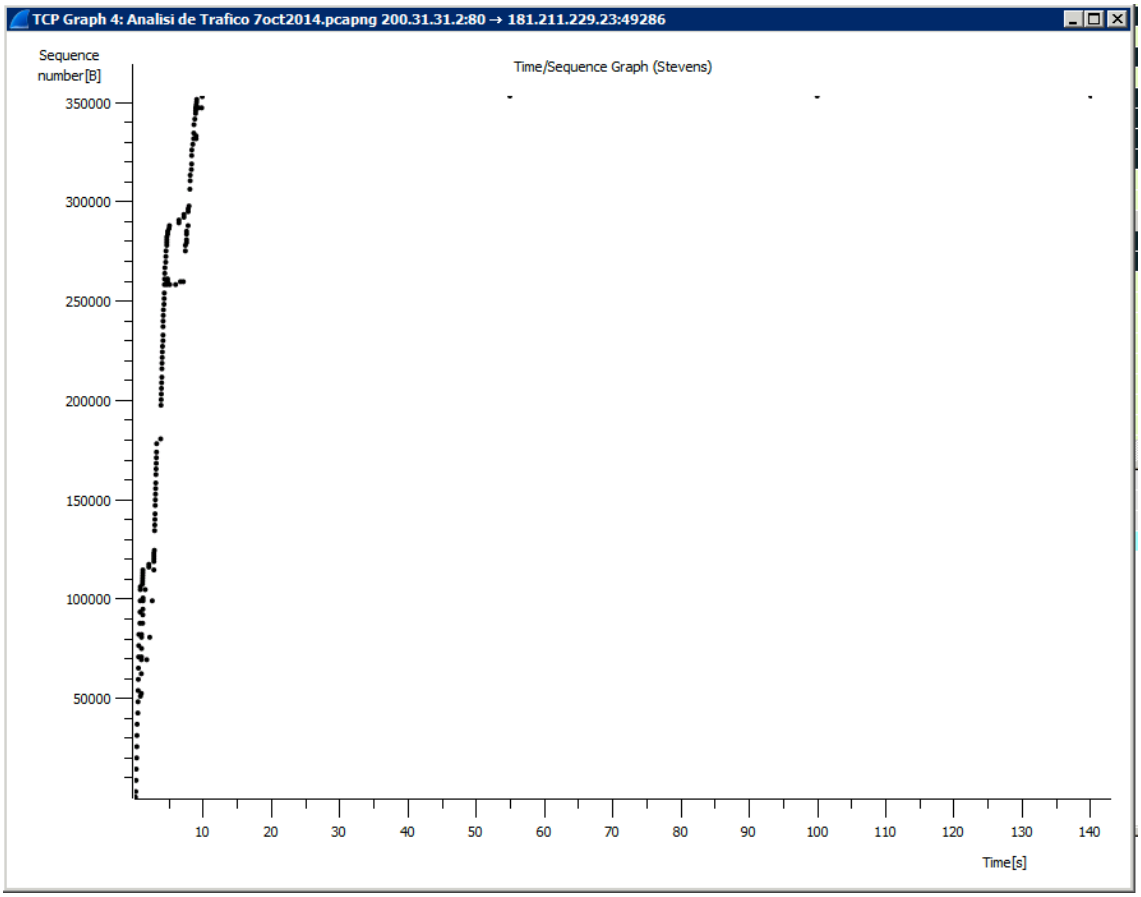


Figura 2.17. Gráficas Wireshark Time Secuencie Graph (Steven), (Nicolalde, 2014)

Si se necesita ver un conjunto de protocolos que han sido separados para ver su proporción respecto al tráfico total se puede utilizar el gráfico IO Graphs. En la figura 2.18 se puede observar el tráfico entrante y saliente del servidor web, se puede observar el tráfico http, ftp y las difusiones broadcast.

[46] Tomado de: (Febrero, 2011)

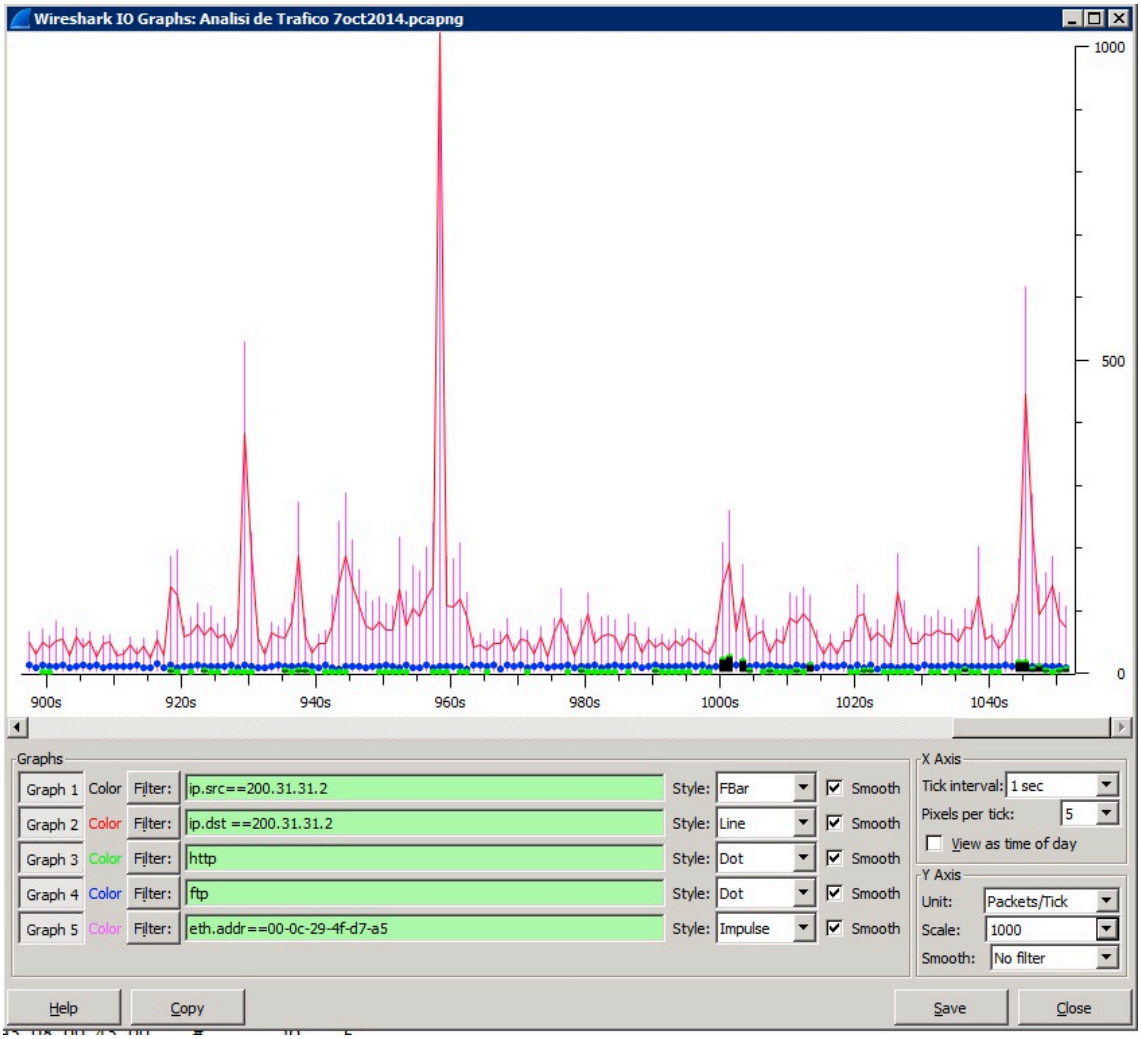


Figura 2.18. IO Graphs, (Nicolalde, 2014)

Luego de haber realizado el análisis del tráfico de la red del Museo QCAZ se ha podido llegar a la conclusión que no existe ninguna anomalía en la misma. No se encontró pruebas de que existan intentos de ataques internos y externos. Además no se ha detectado que el rendimiento de la red empiece a bajar o deje de funcionar, por eso se ha decido que se va a manejar la seguridad de la red del Museo QCAZ con la instalación de un firewall, manteniendo los sistemas operativos actualizados, la definición de virus actualizada, controlando malware y phishing.

2.4. Planificación e implementación de un Firewall

La planificación e implementación del Firewall en el Museo QCAZ, está basada en las recomendaciones de la NIST 800-41 Revision 1 de septiembre del 2009 del Instituto Nacional de Estándares y Tecnología (NIST) del departamento de

comercio de los Estados Unidos, la NIST 800-41 fue escrita por Karen Scarfone y Paul Hoffman y titulada “Guidelines on Firewalls and Firewall Policy”.

De acuerdo a la NIST 800-41 (Scarfone & Hoffman, 2009) la planificación en implementación de un firewall dentro de una organización debe realizarse por fases. La NIST propone cinco fases:

1. **Plan**: hay que identificar todos los requerimientos que la organización considere importantes para que se cumplan las políticas de seguridad de la organización.
2. **Configure**: describe todas las facetas de configuración del firewall. Incluye la instalación de software y hardware, así como las reglas.
3. **Test**: en esta fase se debe evaluar la funcionalidad, el performance, escalabilidad y la seguridad de la solución implementada, esto se debe hacer en un ambiente de pruebas.
4. **Deploy**: una vez que la fase anterior es superada correctamente, se puede desplegar el firewall dentro de la organización.
5. **Manage**: son las actividades de administración del firewall, estas incluyen, mantenimiento de los componentes y soporte para operaciones cuando se necesite incorporar cambios significativos en la solución.

2.4.1. Plan

En la red del Museo QCAZ se han determinado los requerimientos en base a la identificación de las amenazas y vulnerabilidades de los sistemas de información, el impacto que generaría una pérdida de la confidencialidad, integridad y disponibilidad de los servicios y la identificación.

2.4.1.1. Vulnerabilidades de los sistemas de información

En el museo QCAZ existen dos sistemas de información que están disponibles en la web.

En estos sistemas se han podido identificar las siguientes vulnerabilidades:

Injection: el sistema web podría aceptar inyección SQL. Se llego a esta conclusión ya que el sitio web permite subir archivos, pero no controla el formato permitido de los documentos, además no existe un correcto filtrado de la

información que pasa a través de los campos en donde los usuarios pueden ingresar información al sitio web, esto pasa con las dos aplicaciones web.

Broken Authentication and Session Management: el sitio web puede estar expuesto a este tipo de ataque ya que no existe un adecuado control de las sesiones en las aplicaciones que utilizan autenticación.

Missing Function Level Access Control: se ha detectado que en servidor faltan controles, permitiendo a un posible atacante acceder a funciones a las que no debería.

2.4.1.2. Pérdida de la confidencialidad, integridad y disponibilidad de los servicios

El impacto que ocasionaría la perdida de la confidencialidad sería grande en el mundo científico ya que la información que se encuentra en el sitio web corresponde a información recopilada y procesada por científicos de la universidad y es de toda la fauna del Ecuador.

Si se llegara perder la disponibilidad de los servicios el impacto también sería grande, ya que la información que se publica en el sitio web es usada por la comunidad científica, investigadores, profesores, estudiantes y público en general de todo el mundo.

2.4.2. Configure

Esta fase envuelve todas las facetas de configuración del firewall. Estas incluyen la instalación de hardware y software, configuración de políticas, configuración de accesos y la integración del firewall en la red del Museo QCAZ.

Durante el proceso de instalación y configuración solo el administrador encargado de la implementación debería administrar el firewall. Una vez instalado y configurado, los administradores pueden crear las reglas en el firewall.

2.4.3. Test

Una vez instalado y configurado, el firewall debe ser testeado, para el caso del museo QCAZ el firewall fue testeado en una red virtual paralela que no tenía conectividad con la red que está en producción, con la finalidad de no interrumpir el funcionamiento de la misma.

Una vez pasada la prueba, el firewall debe ser introducido en la arquitectura de la red de producción y empezar a funcionar.

Los parámetros que se evaluaron fueron:

- Los usuarios pueden establecer y mantener conexiones a través del firewall.
- Revisar que el tráfico de la red fluya de acuerdo a las políticas de seguridad, es decir, el tráfico no es permitido porque en las políticas de seguridad esta bloqueado.
- La implementación del firewall no interfiera con el funcionamiento de las aplicaciones, sobre todo en las arquitecturas cliente servidor.
- Los accesos permitidos estén configurados de acuerdo a las políticas de seguridad establecidas.
- La implementación del firewall no haya afectado en el performance de la red del museo.

2.4.4. Deploy

Después de pasar las pruebas y corregir todos los problemas encontrados, el firewall es insertado en la arquitectura de la red del museo. Antes de implementar el firewall se debe comunicar a los usuarios para que reporten cualquier novedad.

2.4.5. Manage

Esta es la última fase de la planificación e implementación de un firewall de acuerdo a las recomendaciones de las NIST. Esta fase envuelve el mantenimiento del firewall, políticas, software y otros componentes de la solución. La principal actividad que se debe realizar es el monitoreo del tráfico de la red, actualizar el software del firewall, monitorear los registros y las alertas para identificar amenazas.

Hay que realizar pruebas periódicamente para verificar que las políticas implementadas en el firewall estén funcionando correctamente.

2.4.6. Implementación del Firewall en el Museo QCAZ

Luego de haber realizado el análisis del tráfico de la red y siguiendo las recomendaciones de la NIST 800-41 (Scarfone & Hoffman, 2009), para el Museo se implementará el firewall tomando en cuenta los siguientes aspectos:

2.4.6.1. Configuración del firewall (Untagle)

Para el Museo QCAZ se configurará el Untangle como un "Netwrok Gateway", el cuál estará encargado de filtrar el tráfico que circula por la red, con la finalidad de no ser victimas de intrusos internos o externos. Untangle ofrece varias aplicaciones de las cuales utilizaremos el filtrado web, bloqueo de malware, protección contra información sensible (phishing) y el firewall.

2.4.6.2. Hardware y software a utilizarse

Tratando siempre de que las soluciones planteadas permitan optimizar los recursos existentes en el Museo, con la finalidad de utilizar al máximo los mismos, para la configuración del firewall se utilizará un servidor IBM X3550 que dispone el Museo cuyas características son procesador Intel Xeon 5110 1.60 GHz, 4GB de RAM y 150GB de almacenamiento. El software que se empleará para la configuración del firewall es Untangle[47].

2.4.6.3. Políticas de seguridad

Para la elaboración de las políticas de seguridad a aplicarse en el Museo QCAZ, se tomó en cuenta las recomendaciones de la "Guía para la elaboración de políticas de seguridad" de la Universidad Nacional de Colombia. De acuerdo con esta guía las políticas de seguridad tienen un ciclo de vida mientras estén vigentes. Este ciclo de vida incluye: investigar las posibles fuentes de vulnerabilidad, escribirla, aprobarla, ser difundidas a todos los usuarios de la red, conseguir que los usuarios acaten la política, darle seguimiento, actualizarla y darle de baja cuando haya perdido vigencia.

En la tabla 2.2 de definen las políticas de seguridad a ser aplicadas en el Museo QCAZ y en la tabla 2.3 los procedimientos.

[47] Untangle es un network Gateway libre diseñado específicamente para pequeñas empresas, entre las muchas aplicaciones que ofrece usaremos para el museo el filtrado web, el firewall, boqueo de tráfico malicioso, protección contra información sensible (phishing).

Definición de la política	Quién Autoriza	Quién Propone	Quiénes acatan	Indicadores de cumplimiento	Solicitar excepcione
Garantizar seguridad en la información que se descargan del internet.	Director	Dep. de informática	Todos los usuarios de la red	Navegan por sitios permitidos	Enviar solicitud departament de informá indicando el web al que d ingresar.
Garantizar confidencialidad, integridad y disponibilidad de la información que se encuentra en las bases de datos.	Director	Dep. de informática	Todos los usuarios de la red	Monitorear el valor de las variables que llevan información desde el sitio web hacia la parte lógica. Escanear los puertos que se encuentran abiertos.	Enviar solicitud departament de informá indicando el web al que d ingresar.
Garantizar la seguridad de la información	Director	Dep. de informática	Encargad o de backups	Backups en medios magnéticos.	No aplica
Educación y capacitación constante sobre las políticas del museo.	Director	Dep. de informática	Todos los usuarios de la red	Bitácoras de capacitación.	No aplica

Tabla 2.2 Definición de las políticas de seguridad, (Nicolalde, 2014)

Política	Estándar	Mejor práctica	Procedimientos	Guía
Garantizar seguridad en la información que se descargan del internet.	La información que se descargan pasa por un antivirus y malware aprobados por la universidad.	Configurar de manera adecuada la seguridad del navegador de internet.	Bloquear sitios web en el firewall.	Se recomienda a los usuarios no bajarse archivos de sitios no confiables.
Garantizar confidencialidad, integridad y disponibilidad de la información que se encuentra en las bases de datos.	Llevar un control adecuado de las sesiones que se inician en el sitio web con autenticación, y de los datos que los usuarios pueden ingresar en los campos del sitio web.	Validar los campos del sitio web. Crear contraseñas seguras. Escanear frecuentemente los puertos.	Establecer tiempos para caducidad de la sesión. No permitir que los usuarios ingresen cualquier tipo de información en los campos que se encuentran disponibles en el sitio web. Instalar un malware y mantenerlo actualizado en el servidor. Bloquear los puertos que no se necesiten o que faciliten el acceso a la red por parte de intrusos.	Se recomienda a los usuarios crear contraseñas seguras.
Garantizar la seguridad de la	Políticas de backups.	Realizar backups	Crear tareas programadas para que	Verificar que el sistema de backups esté

información		diariamente.	realicen respaldos de forma automática.	funcionando adecuadamente.
Educación y capacitación constante sobre las políticas del museo.	Estructuración de cursos de capacitación	Capacitación permanente.	Dictar capacitaciones presenciales o virtuales.	Elaborar una guía con las políticas del museo.

Tabla 2.3. Procedimientos para aplicar las políticas de seguridad, (Nicolalde, 2014)

2.4.6.4. Red del Museo QCAZ

En la figura 2.19 se puede observar la configuración de la red del QCAZ. Entre la conexión a internet y el switch central se ha colocado el network Gateway (firewall).

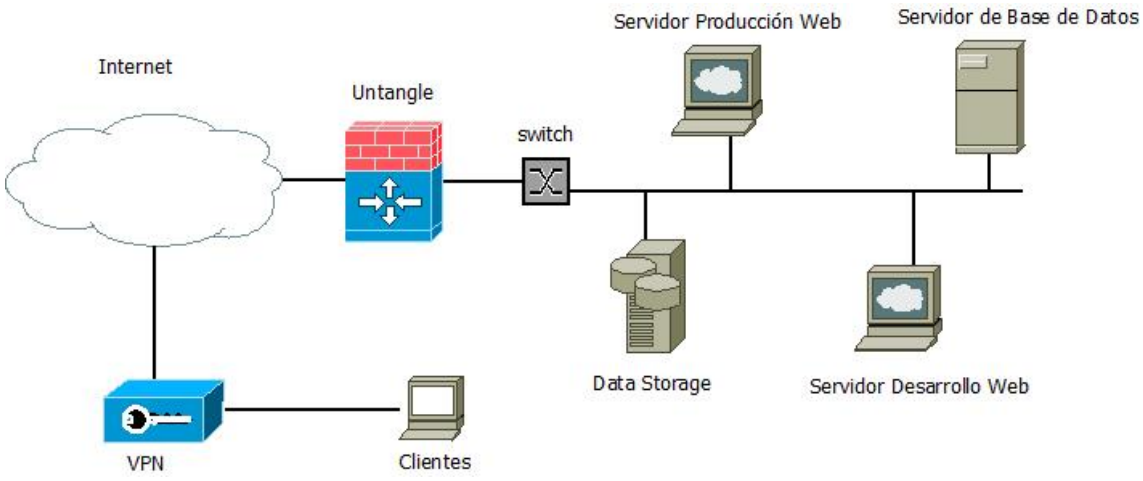


Figura 2.19. Red del Museo QCAZ, (Nicolalde, 2014)

CAPÍTULO III

APLICACIONES

3. Aplicaciones

3.1. Instalación y configuración del sistema de virtualización con VMWare para el Museo QCAZ.

Para instalar la infraestructura virtual en el Museo QCAZ, se utilizó la tecnología proporcionada por VMware vSphere 5 Hypervisor con licencia para 2 CPUs físicos (número de cores indefinidos por CPU). Por ser una licencia gratuita presenta el limitante que reconoce hasta 32 GB de RAM.

Esta tecnología VMware se instaló sobre un servidor Hp ProLiant DL385 G6 con las siguientes características:

- Dos procesadores Six-Core AMD Opteron (tm) Processor 2431
- 12 CPUs x 2,4 GHz
- 32 GB de memoria RAM
- 2 datastorage de 1TB cada uno.

En la figura 3.1 se puede observar el sumario de las características del servidor.

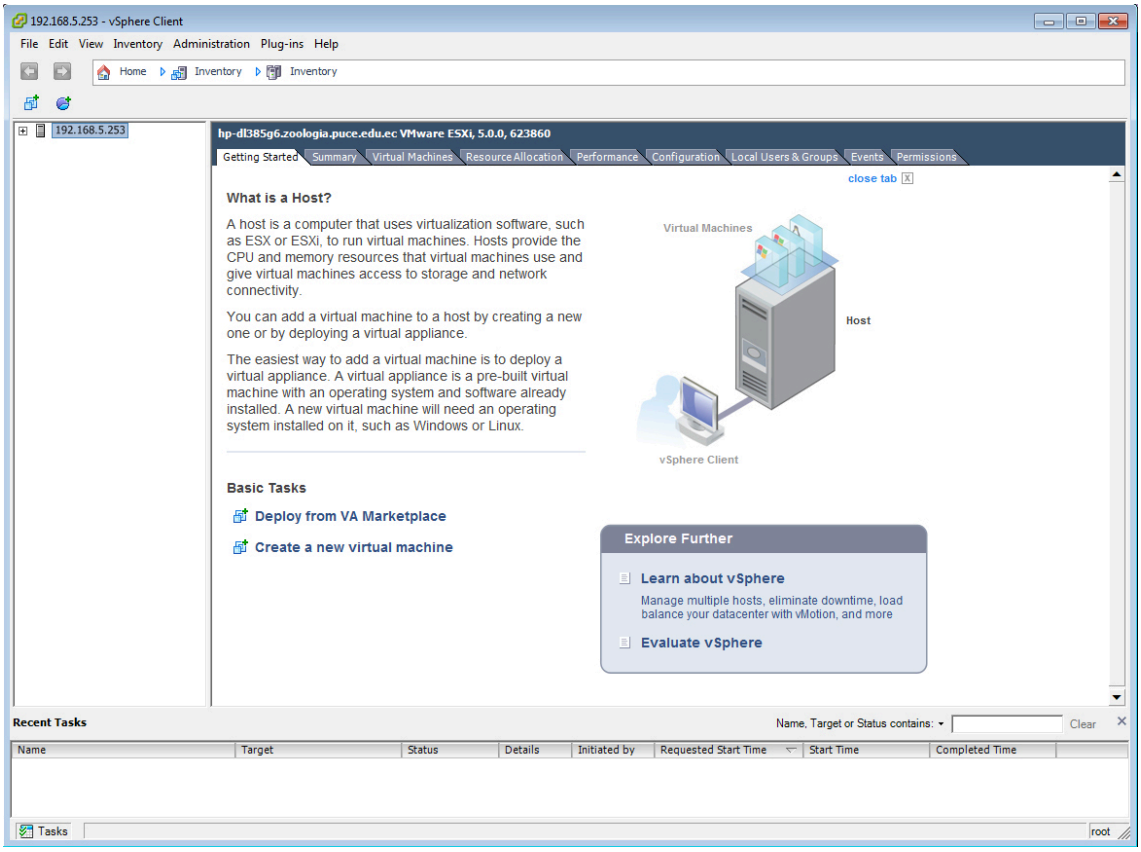
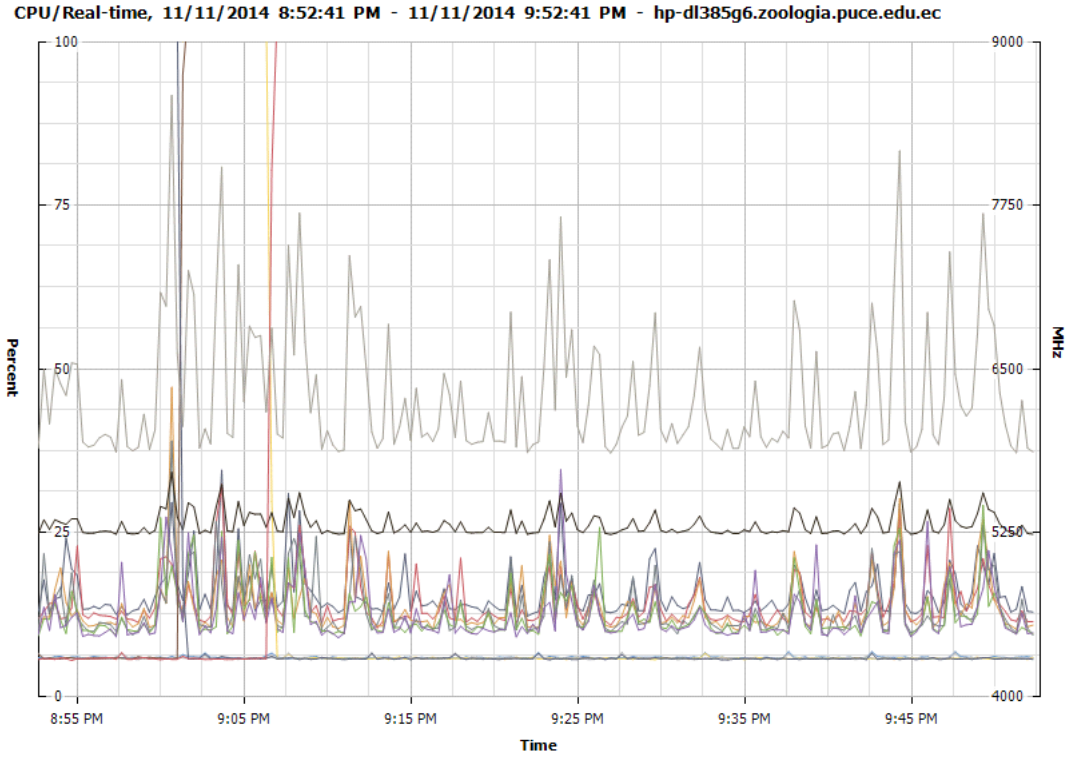


Figura 3.1. vSphere Client[48]. Summary, (Nicolalde, 2014)

En la figura 3.2 se puede observar las estadísticas acerca del rendimiento del servidor.

[48] vSphere Client: software que permite administrar las máquinas virtuales que se están desplegando en el hypervisor Esxi.



Performance Chart Legend

Key	Object	Measurement	Rollup	Units
	0	Usage	average	Percent
	1	Usage	average	Percent
	2	Usage	average	Percent
	3	Usage	average	Percent
	4	Usage	average	Percent
	5	Usage	average	Percent
	6	Usage	average	Percent
	7	Usage	average	Percent
	8	Usage	average	Percent
	9	Usage	average	Percent
	hp-dl385g6.zoologia.puce.edu.ec	Usage	average	Percent
	hp-dl385g6.zoologia.puce.edu.ec	Usage in MHz	average	MHz
	10	Usage	average	Percent
	11	Usage	average	Percent

Figura 3.2. Servidor performance. CPU, (Nicolalde, 2014)

En la figura 3.2 se puede observar que el rendimiento del servidor es bastante aceptable, en ningún momento llega a saturarse el uso del CPU (con todos los servidores encendidos el uso promedio no sobrepasa el 75%), con lo cuál se puede demostrar que un sistema virtualizado con VMware usa hasta en un 90% el

hardware del servidor, sin que exista una saturación en la utilización de los recursos.

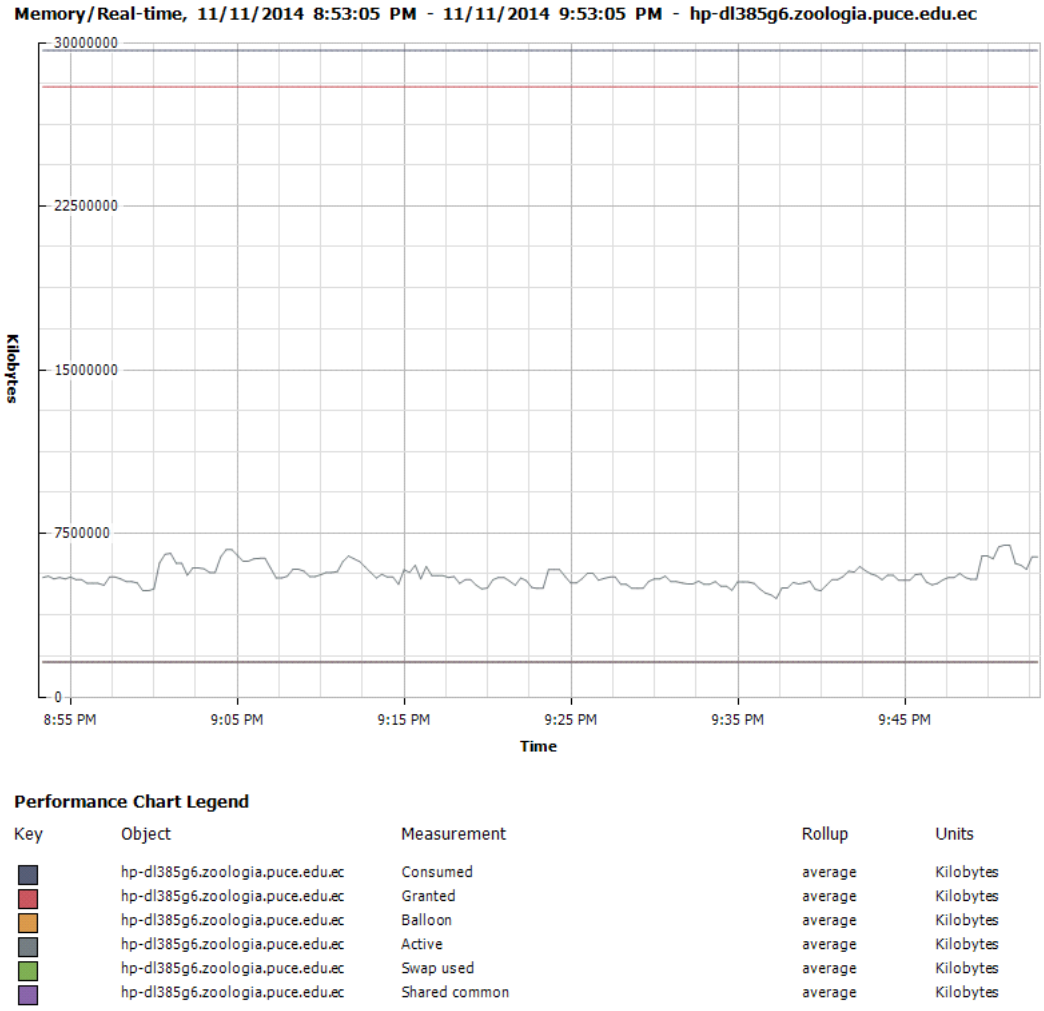


Figura 3.3. Servidor performance. Memory, (Nicolalde, 2014)

En la figura anterior, se puede observar la utilización de la memoria, en el caso del servidor del Museo están utilizados 28 GB de los 32 disponibles. Se puede

observar que la memoria activa no sobrepasa los 8 GB lo que garantiza que no existen problemas de rendimiento en el servidor.

La instalación paso a paso de VMware vSphere ESXi 5 se la puede observar en el anexo 1.

3.2. Instalación y configuración de los servidores para el Museo QCAZ

Para el correcto funcionamiento de los requerimientos del Museo QCAZ, es necesario la instalación de los siguientes servicios:

i. Un servidor con el sistema operativo Windows 2008 server con el servidor web IIS[49] 7 instalado, con soporte para PHP, instaladas las bases de datos SQLServer 2012 Express y MySQL 5. Este servidor es para producción.

ii. Un servidor con el sistema operativo Windows 2008 server con el servidor web IIS 7 instalado, con soporte para PHP, instaladas las bases de datos SQLServer 2012 Express y MySQL 5. Este servidor es para desarrollo.

iii. Un servidor Network Gateway, en el caso del Museo QCAZ con Untangle, este debe tener configurados: firewall, malware y phishing.

iv. Un servidor con el sistema operativo Redhat 6.0 con Apache, ftp y servidor de aplicaciones Jboss instalados. Para pruebas también debe estar el servidor de aplicaciones Glassfish, el MySql 5 y el Postgres 9. Este servidor es para las aplicaciones desarrolladas en java.

En la figura 3.4 se puede observar a los servidores mencionados en los puntos anteriores.

[49] IIS: Internet Information Services

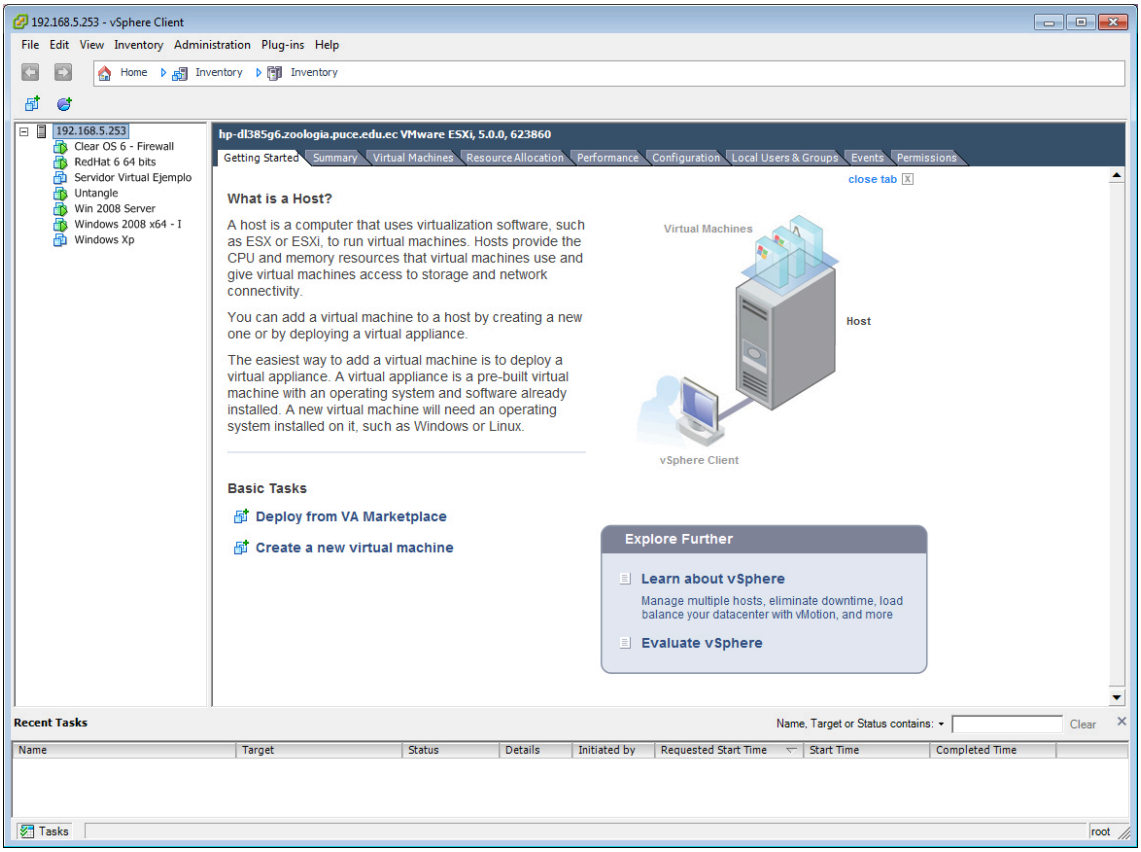


Figura 3.4. Servidores virtuales del Museo QCAZ, (Nicolalde, 2014)

A continuación se describen los pasos que se deben seguir para instalar un nuevo servidor virtual sobre el hypervisor:

Primero hay que colocarse sobre el servidor, hacer clic con el botón derecho del mouse y seleccionar la opción “New Virtual Machine”

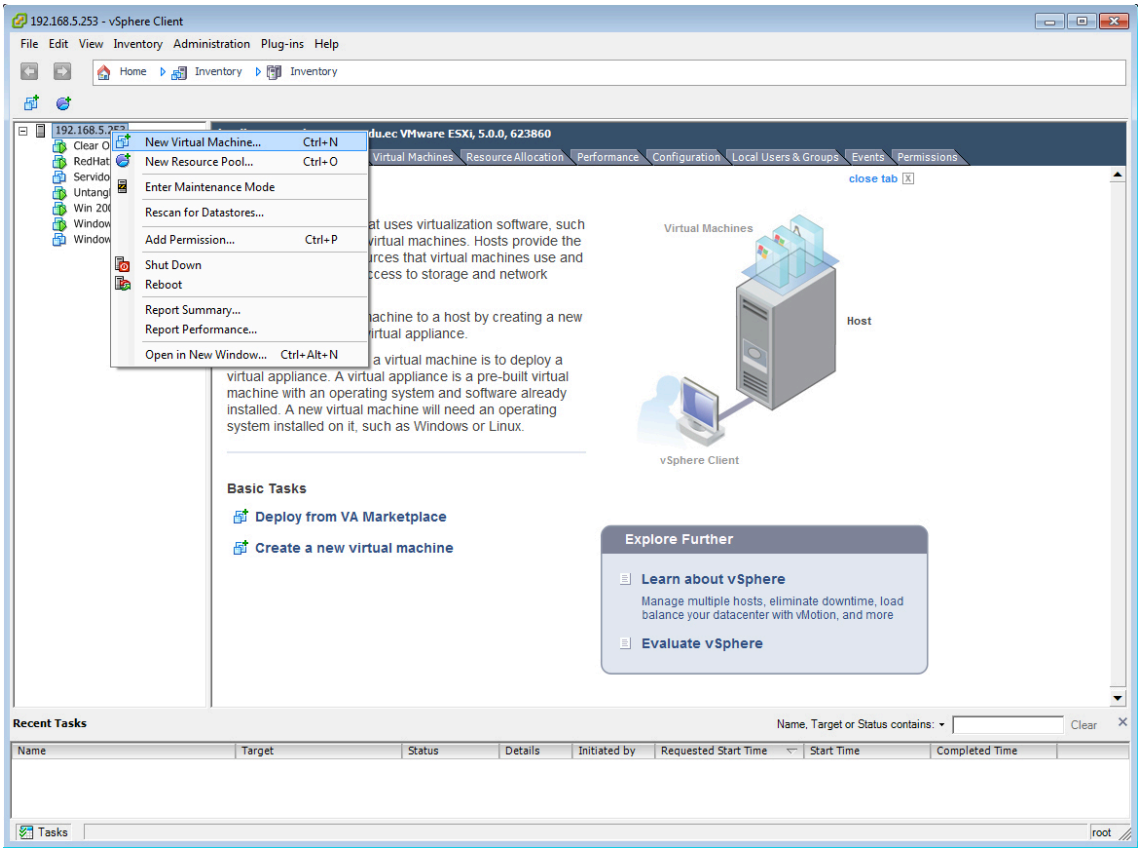


Figura 3.5. Crear una nueva máquina virtual, (Nicolalde, 2014)

A continuación, hay que seleccionar la opción “Custom”, en la siguiente ventana hay que colocar el nombre de la máquina virtual y hacer clic en “Next”.

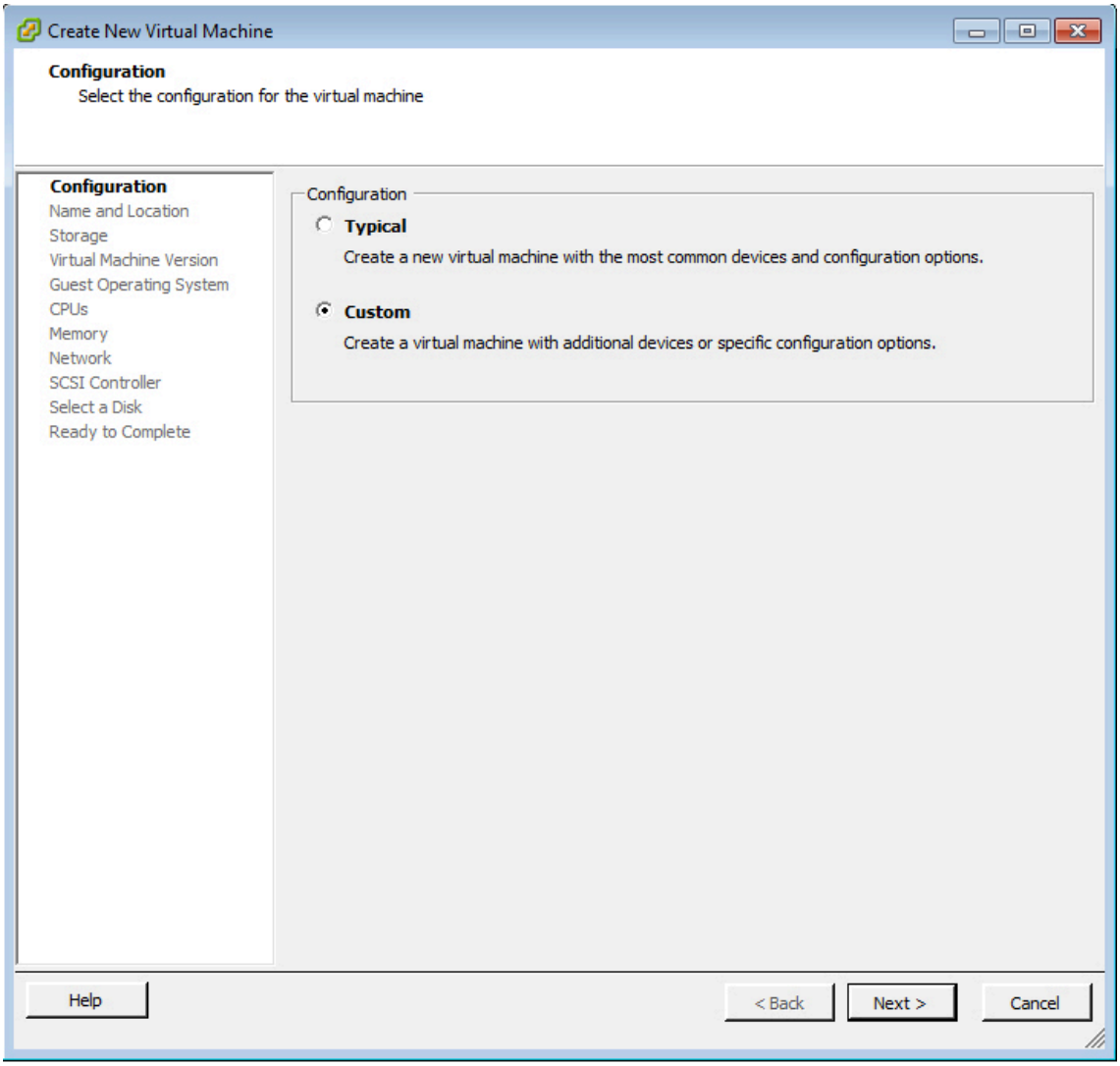


Figura 3.6. Crear una nueva máquina virtual. Tipo de instalación, (Nicolalde, 2014)

Luego hay que seleccionar el datastorage donde se desea guardar los archivos de la máquina virtual, en el caso del Museo QCAZ el servidor dispone de dos datastorage, para el ejemplo se almacenará en el datastorage2.

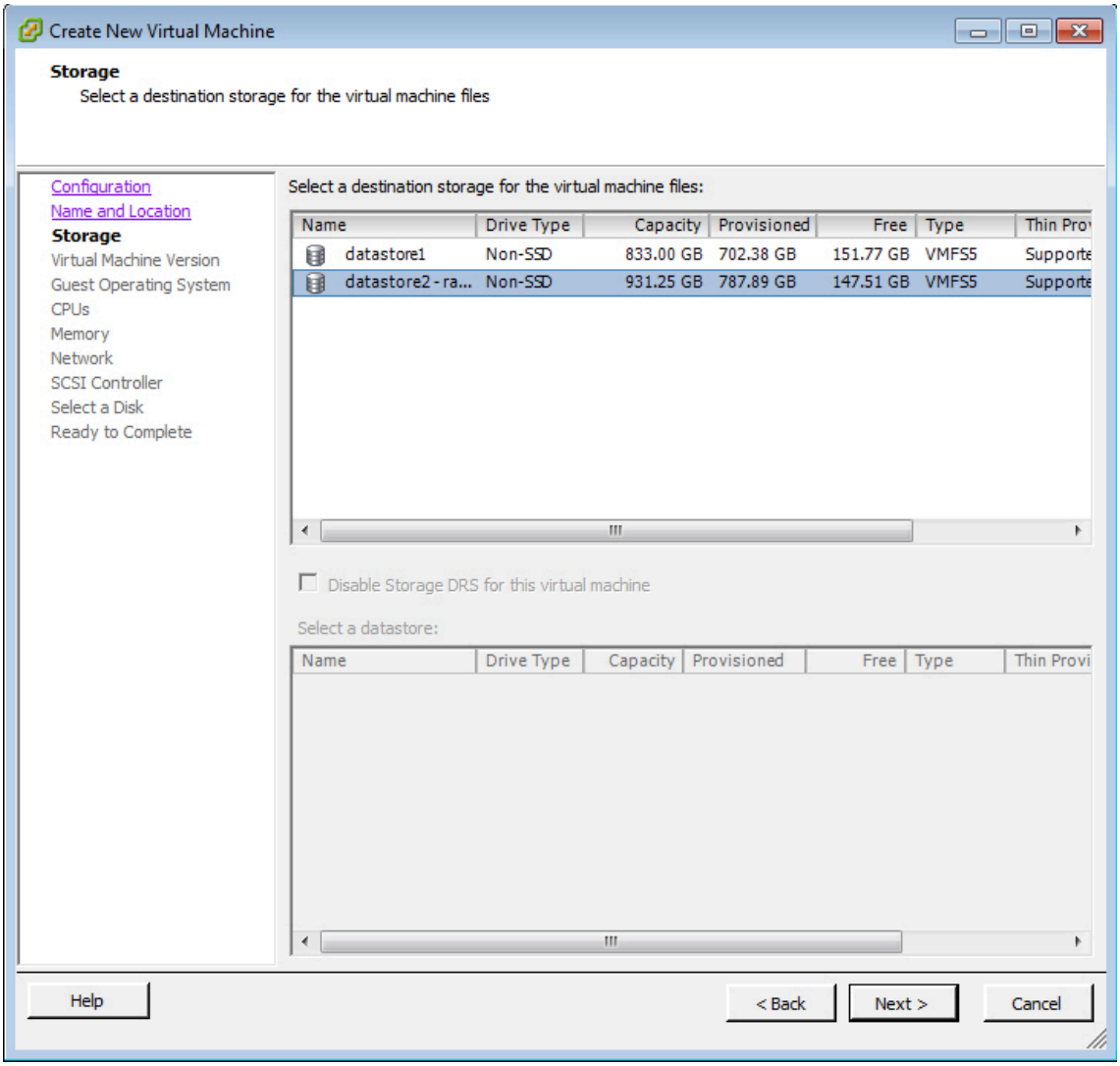


Figura 3.7. Crear una nueva máquina virtual. Seleccionar datastorage, (Nicolalde, 2014)

Después se debe seleccionar la versión de la máquina virtual a utilizarse, para el caso del Museo la versión 8.

En la ventana que aparece hay que seleccionar el sistema operativo que se va a instalar con su respectiva versión, para el ejemplo es Windows y la versión Microsoft Windows Server 2008 R2 (64 bits).

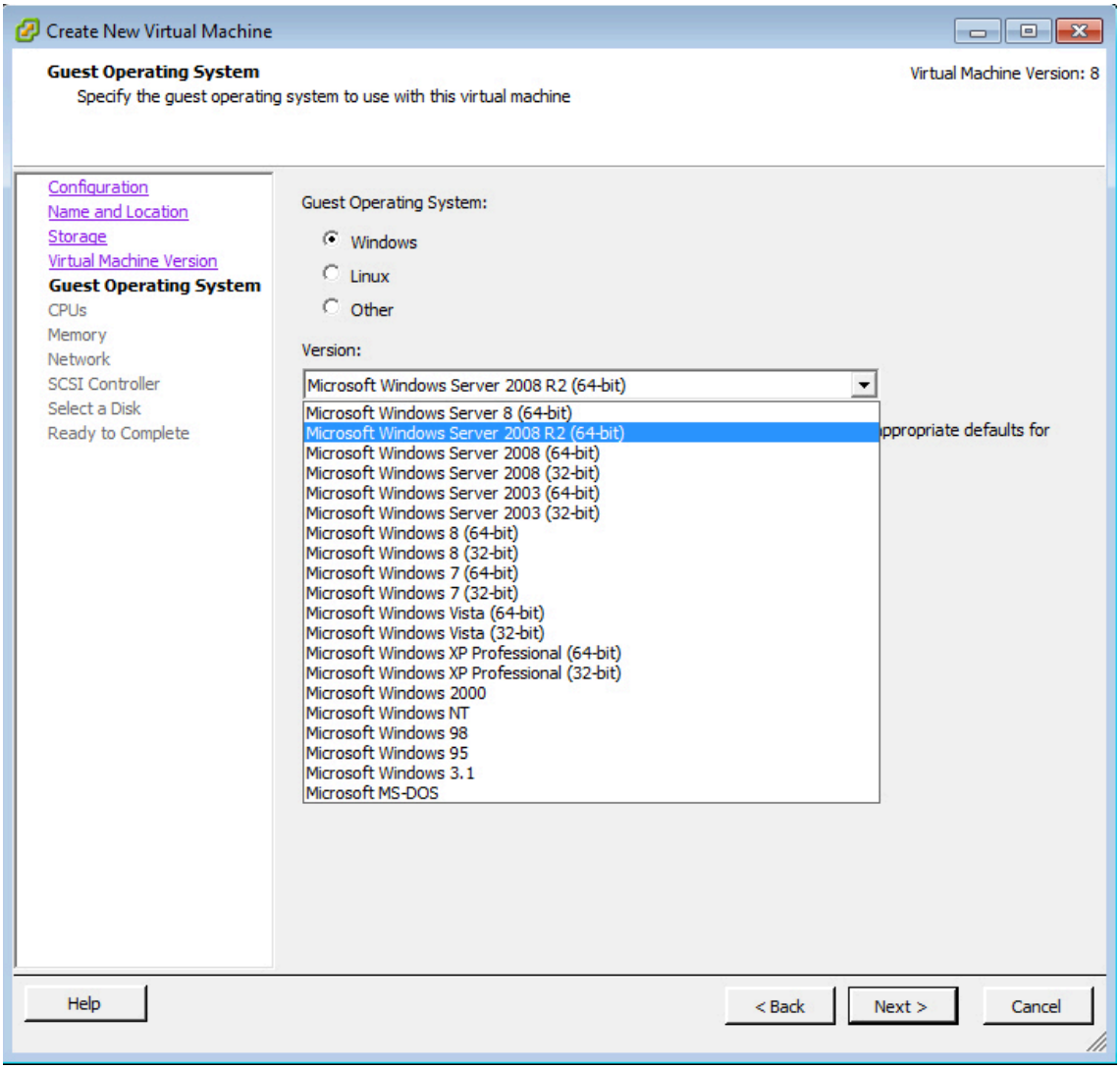


Figura 3.8. Crear una nueva máquina virtual. Seleccionar sistema operativo, (Nicolalde, 2014)

Luego hay que configurar los CPUs que se necesitan para el servidor virtual, se puede seleccionar el número de sockets virtuales y el número de cores por cada socket (no hay que olvidar que el número total de cores es de 12 para no sobrepasar la capacidad). Para el caso del ejemplo se deja 1 socket virtual y 2 cores por el socket.

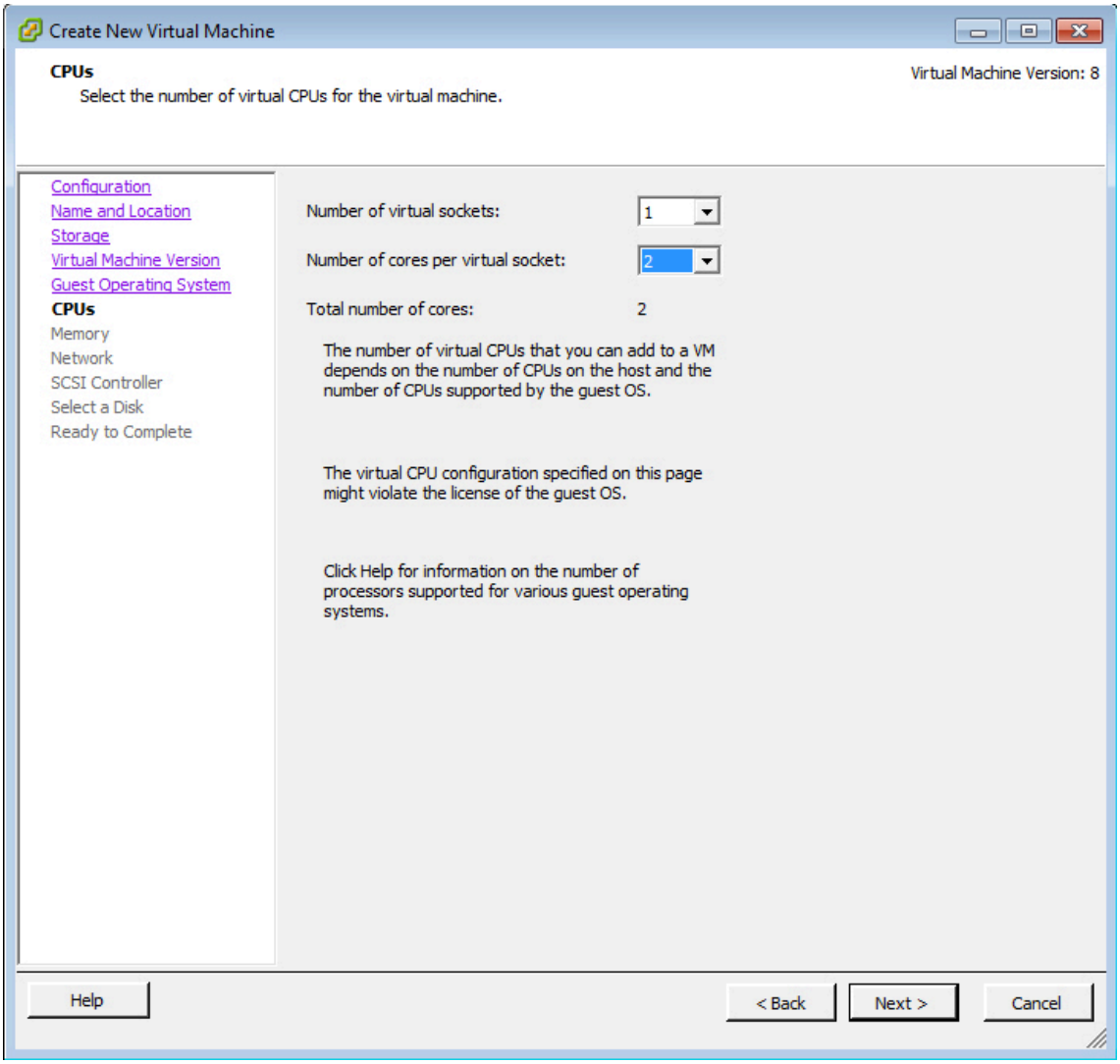


Figura 3.9. Crear una nueva máquina virtual. Configuración CPUs, (Nicolalde, 2014)

A continuación se debe configurar la cantidad de memoria RAM que se le quiere asignar al servidor virtual (no hay que olvidar que la cantidad total de memoria es de 32 GB). Para el ejemplo se toman 4 GB.

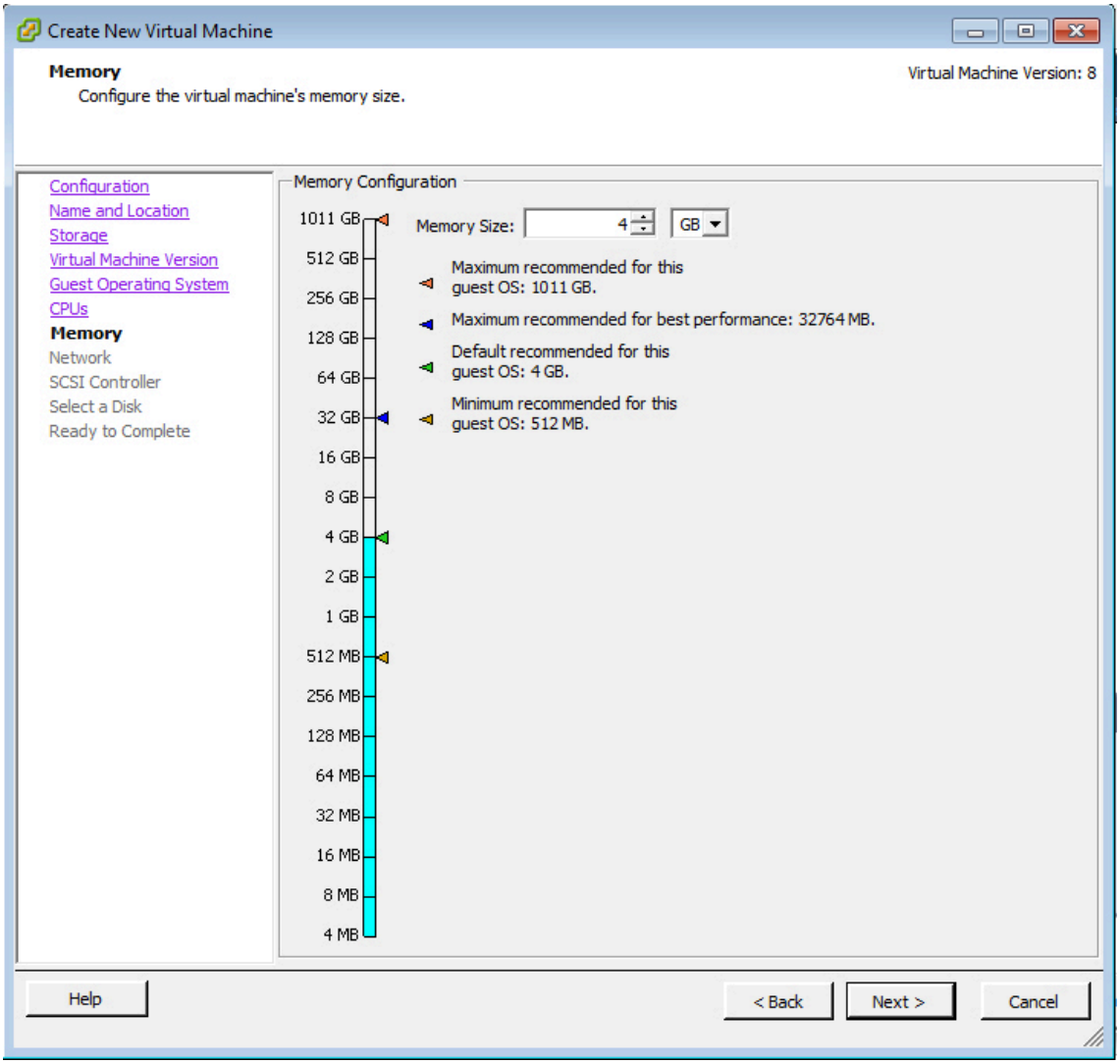


Figura 3.10. Crear una nueva máquina virtual. Configuración memoria RAM, (Nicolalde, 2014)

Después se debe configurar las conexiones de red que tendrá el servidor virtual, para el ejemplo 2.

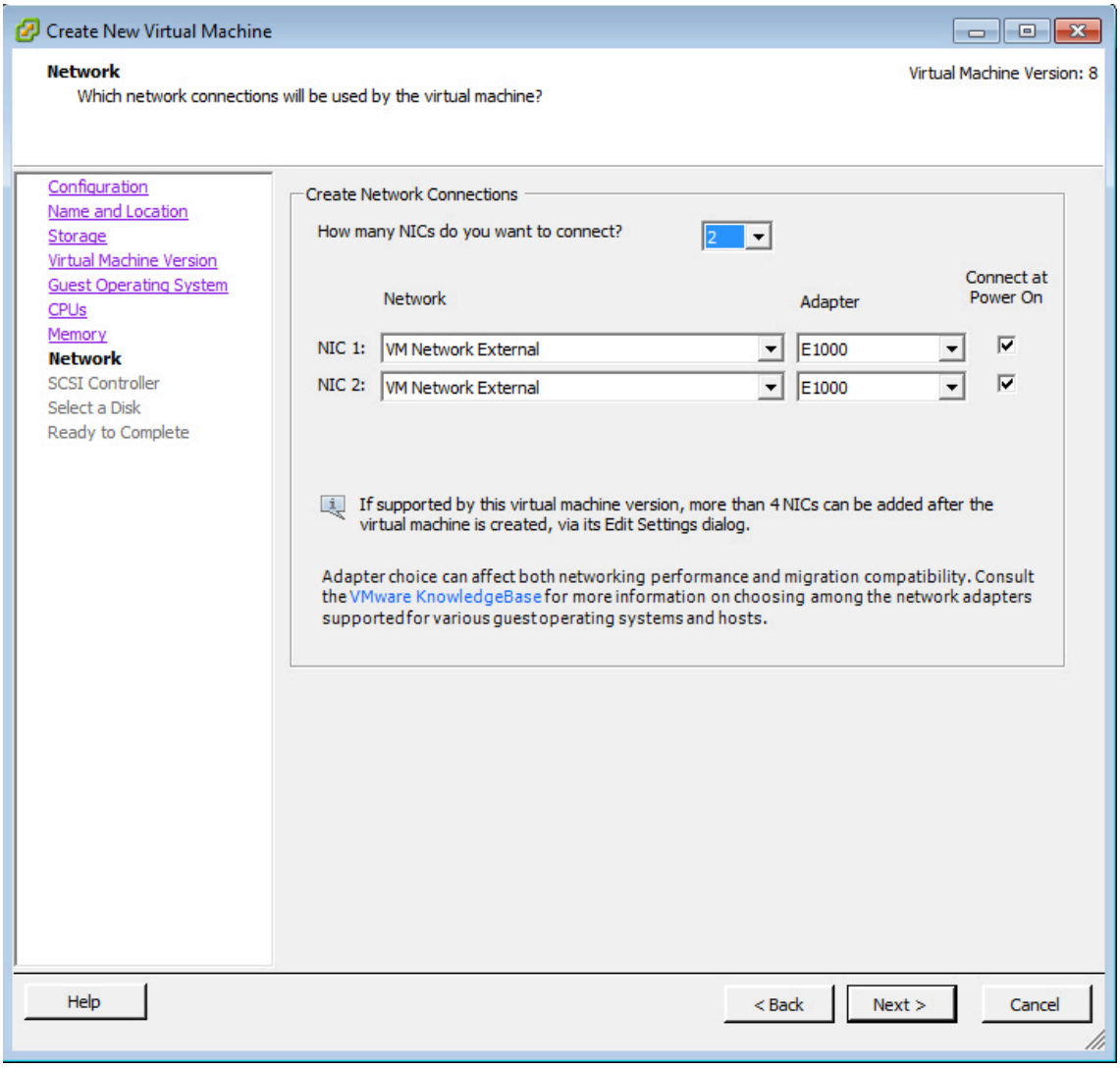


Figura 3.11. Crear una nueva máquina virtual. Configuraciones de Red, (Nicolalde, 2014)

A continuación se debe seleccionar el tipo de disco a usarse, puede ser: un nuevo o un existente, para el ejemplo, se usará un nuevo.

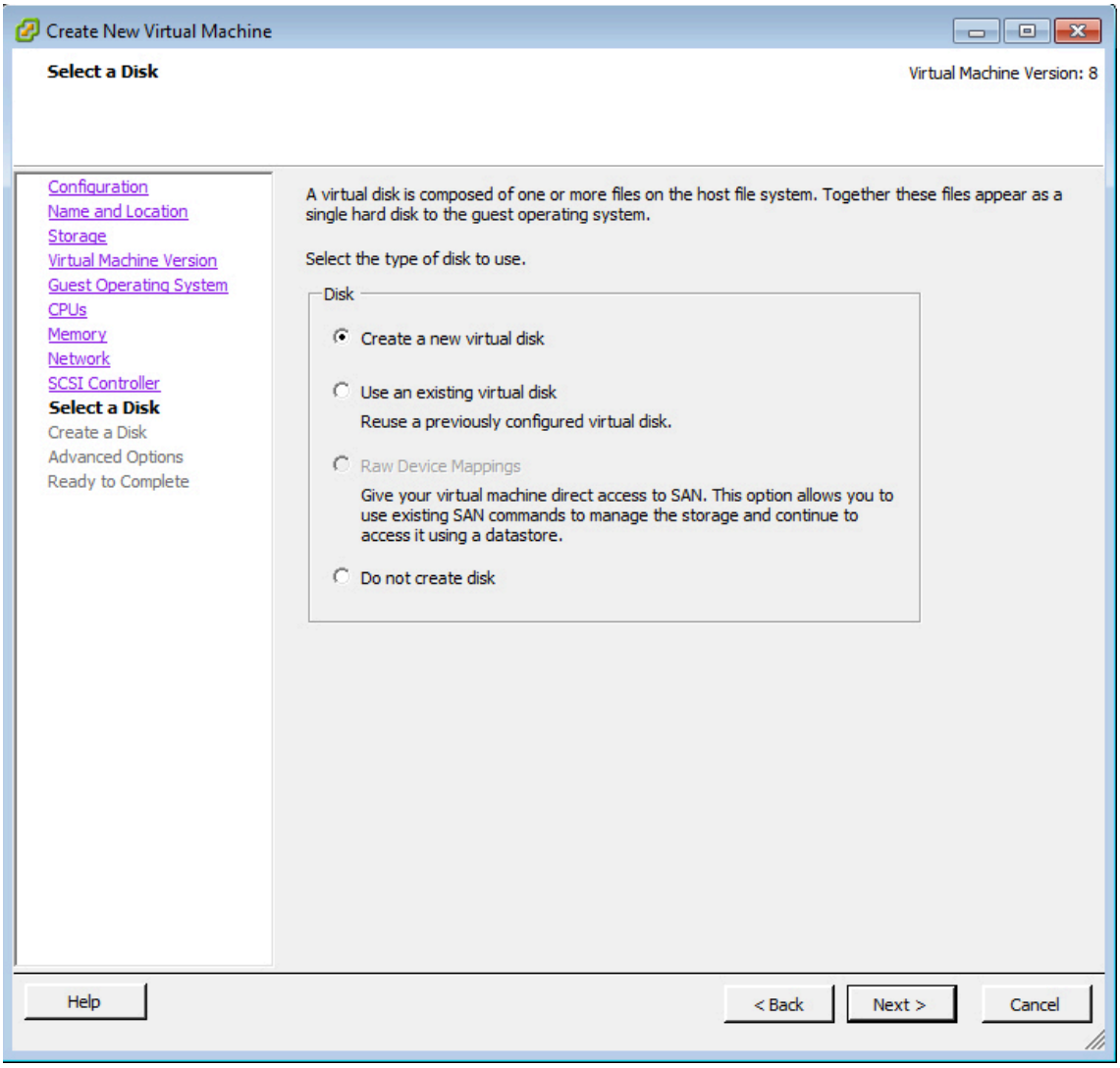


Figura 3.12. Crear una nueva máquina virtual. Tipo de disco, (Nicolalde, 2014)

Se debe establecer la capacidad del disco duro de la máquina virtual (tamaño recomendable hasta unos 750 GB para no tener problemas cuando se requiera hacer respaldos de las máquinas virtuales)

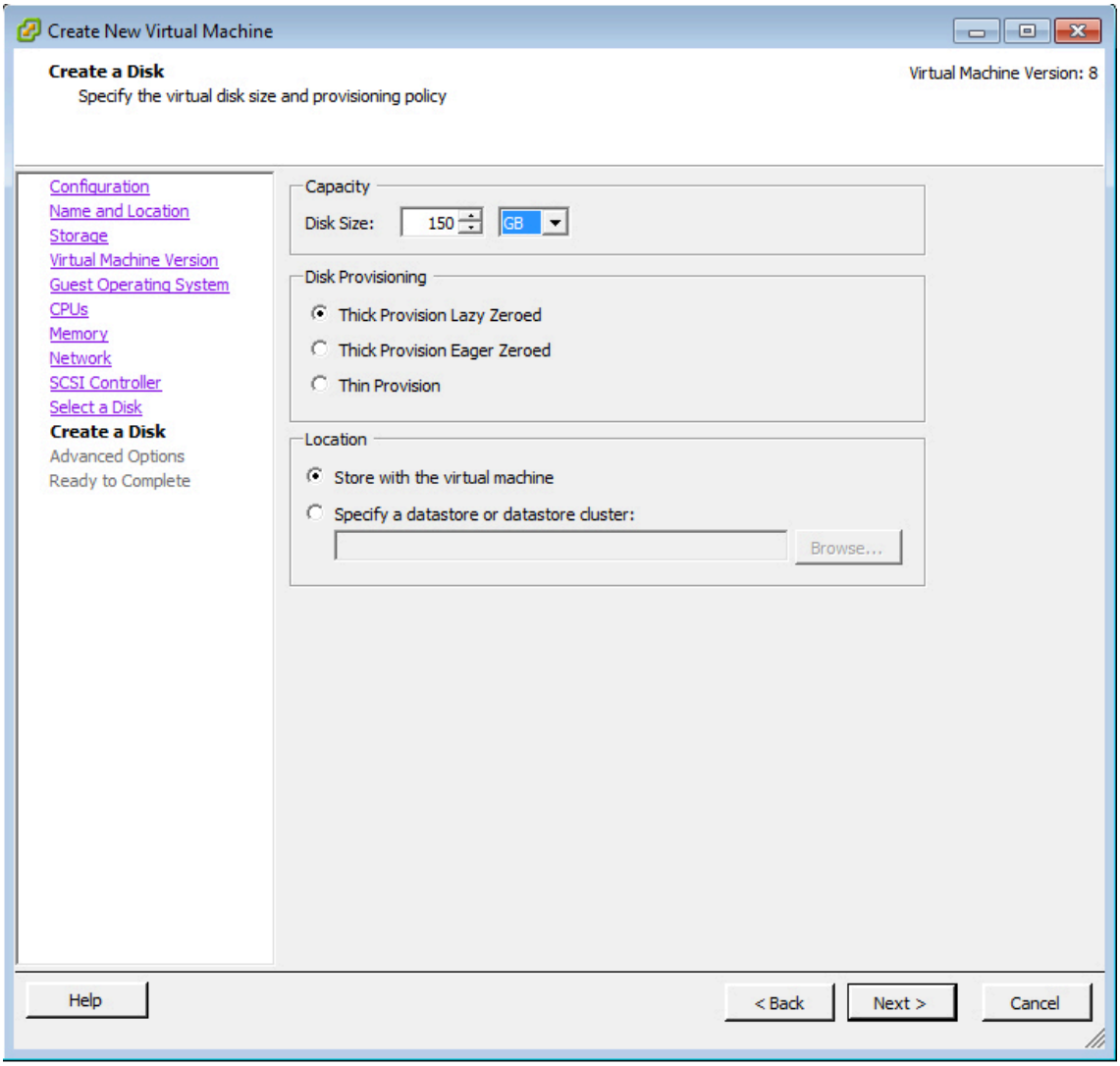


Figura 3.13. Crear una nueva máquina virtual. Configurar capacidad de disco, (Nicolalde, 2014)

Finalmente, aparece una ventana en donde se puede observar las propiedades de la máquina virtual que se acaba de crear y además si se requiere se pueden modificar las mismas.

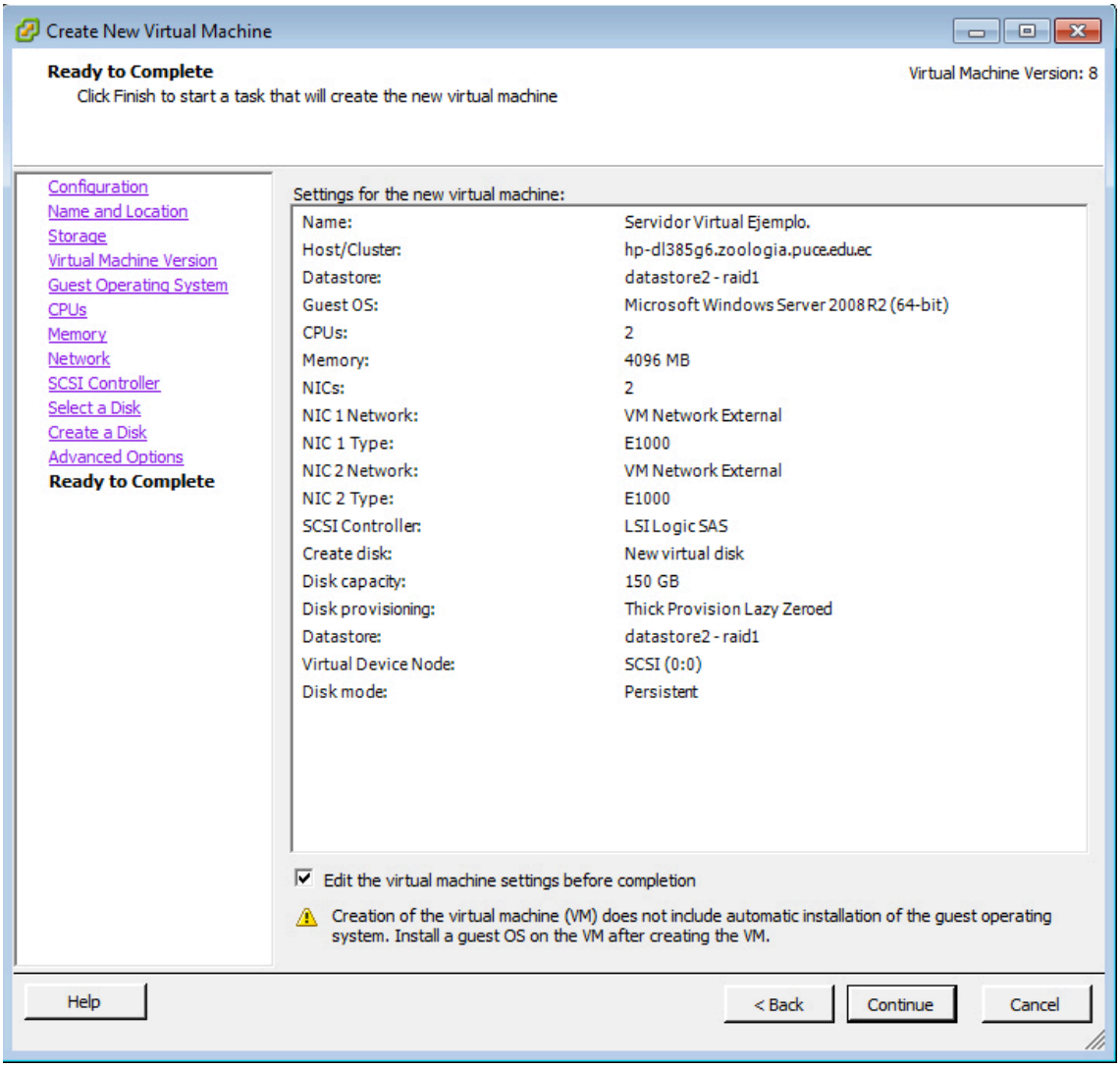


Figura 3.14. Crear una nueva máquina virtual. Propiedades de la máquina virtual, (Nicolalde, 2014)

Una vez creado el servidor, hay que instalar el sistema operativo, tal como si se lo hiciera sobre un servidor físico.

3.3. Instalación y configuración de un Network Gateway (pasarela de red).

En la figura 3.15 se puede observar la configuración de la red del Museo QCAZ luego de instalar y configurar el “Network Gateway”, el network gateway tiene dos tarjetas de red, una externa con la ip 200.31.31.3 la otra interna con la ip 192.168.1.1 como se indica en la figura 3.16.

La tarjeta externa es la que se expone a internet, mientras que la interna es la puerta de enlace para que los servidores que se encentran en la red local puedan salir al internet.

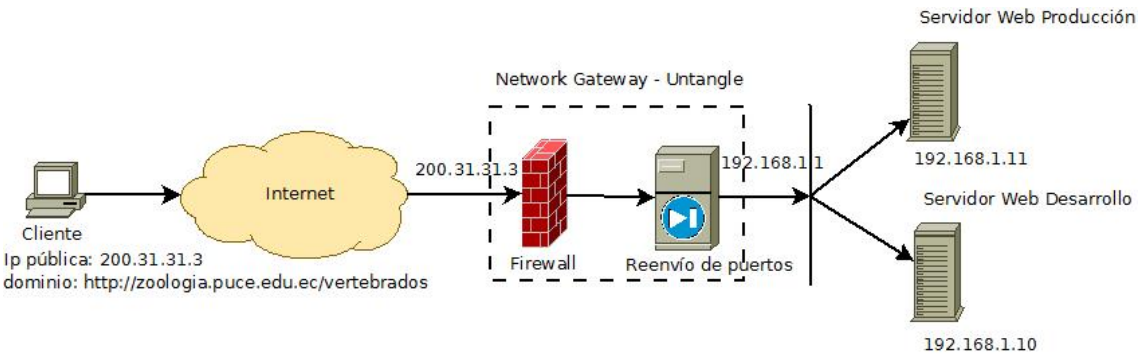


Figura 3.15. Red del Museo QCAZ, (Nicolalde, 2014)

Cabe señalar que para el Museo se ha seleccionado como software para hacer las funciones de Network Gateway a Untangle, como se puede observar en la figura anterior, el Untangle realiza dos tareas fundamentales para garantizar la seguridad del tráfico de la red: la primera es hacer las funciones de un firewall (ver figura 3.18) y la segunda realiza el reenvío de puertos desde la ip pública hacia las ips privadas de la red (ver figura 3.17), de este modo los servicios que se encuentran brindando los servidores desde la red local pueden ser expuestos al internet.

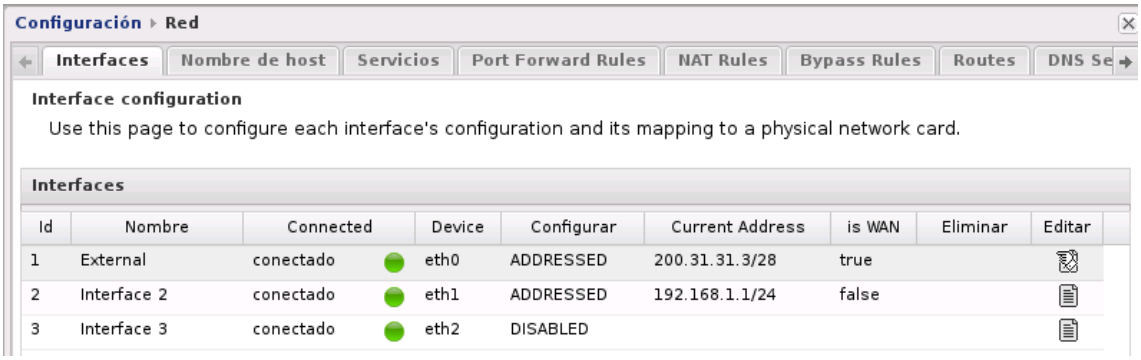


Figura 3.16. Interfaces de red instaladas en el network Gateway, (Nicolalde, 2014)

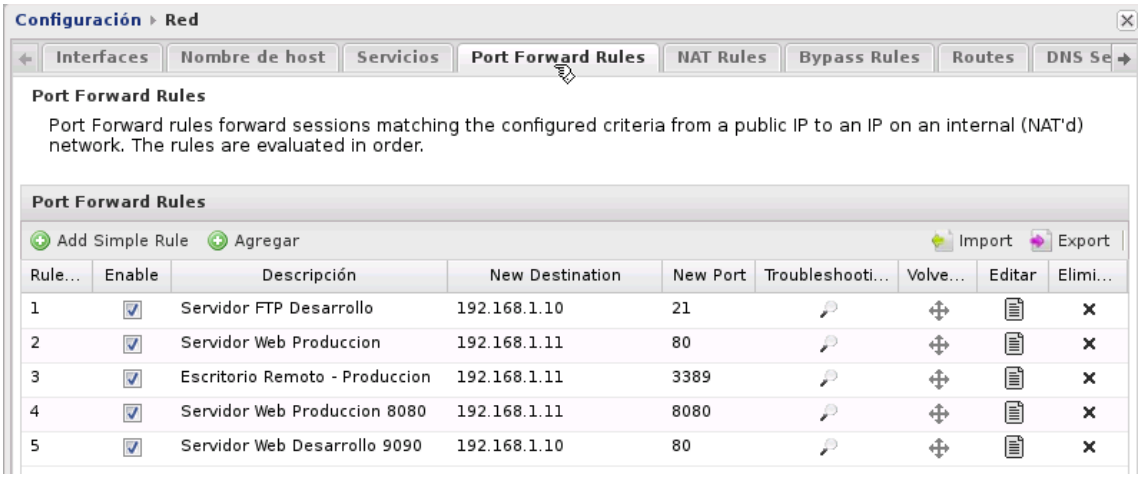


Figura 3.17. Reenvío de puertos, (Nicolalde, 2014)

Para el reenvío de puertos desde la ip pública hacia las ips privadas, se debe tener en cuenta ciertos parámetros, tal como se indica en la tabla 3.1.

Port forward rules	
Destination address	200.31.31.3
Destined local	
Protocolo	TCP and UDP
Destination port	9090
Forward to the following location	
New destination	192.168.1.11
New port	3389

Tabla 3.1. Reglas para reenvío de puertos, (Nicolalde, 2014)

Destination address, aquí hay que colocar la dirección ip pública a donde se conectarán los clientes.

Protocolo, se debe indicar si la conexión que se va a realizar a través del puerto es orientada a la conexión TCP o no UDP.

Destination port, va el puerto desde donde se hace la petición del servicio, ejemplo: http://200.31.31.3:9090, es recomendable al menos en los puertos

críticos realizar un alias con otro puerto de modo que los atacantes no tengan acceso directo al puerto que se encuentra abierto en el servidor.

New destination, es la dirección ip del servidor interno, desde donde se exponen los servicios (a donde se va a allegar).

New port, es el puerto real del servidor interno que esta abierto para exponer los servicios.

En la tabla 3.1., se muestra la configuración de la regla que permite el uso de escritorio remoto desde cualquier cliente. El cliente hace la petición de conexión desde un Remote Desktop Client colocando los siguientes datos:

Ip: 200.31.31.3:9090

User: Nombre_usuario

Pass: password

Cuando llega esta petición al network Gateway, este primero verifica que el puerto se encuentre abierto en el Firewall, luego que exista la regla de reenvío de puertos para el puerto de la petición del cliente, que en este caso es el 9090, se confirma en la tabla de reglas que si existe una regla para ese puerto y se envía la petición hacia la ip interna 192.168.1.11 por el puerto 3389 que corresponde al puerto que permite el acceso al escritorio remoto.

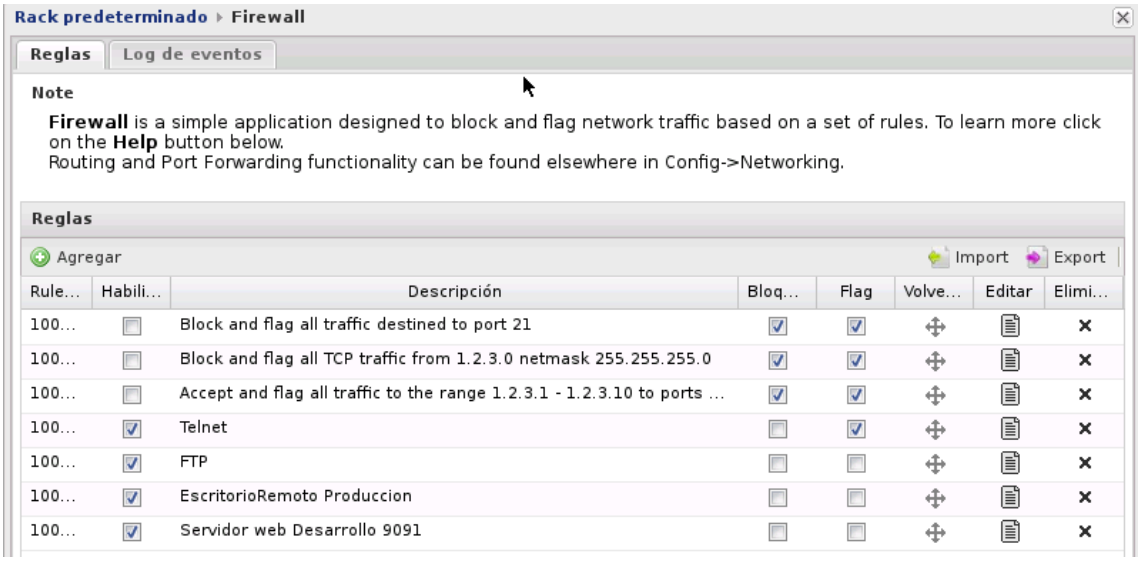


Figura 3.18. Firewall, (Nicolalde, 2014)

Para crea una regla en el firewall también hay que tomar en cuenta algunos parámetros como se muestra en la tabla 3.2.

Firewall rules	
Puerto de destino	9090
Acción	Abierto

Tabla 3.2. Regla para el firewall, (Nicolalde, 2014)

El puerto destino indica justamente el puerto que debe verificarse si esta abierto o bloqueado, en caso de estar bloqueado ya no permite el paso de la conexión.

También se filtro el tráfico de la red a través de la configuración de dos herramientas que trae consigo el Untangle que ayudan a evitar ataques de tipo phishing y actividad maliciosa.

Para prevenir los ataques phishing se habilitó el Phish Blocker.

Para prevenir la actividad maliciosa de la red, se instaló y habilitó el “Untangle Instrusion Prevention” (Ver figura 3.19)

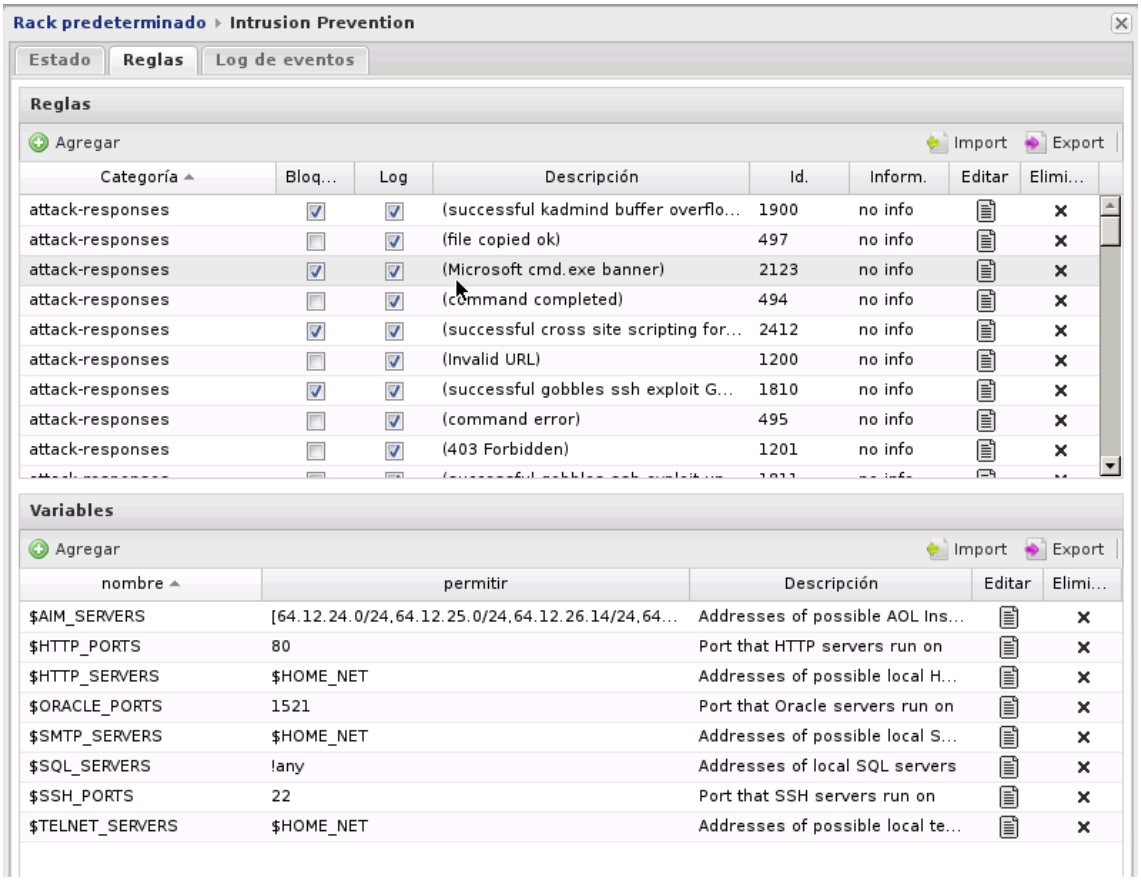


Figura 3.19. Untangle Instrusion Prevention, (Nicolalde, 2014)

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4. Conclusiones y recomendaciones

4.1. Conclusiones

- Un data center tienen que ser diseñado y construido de acuerdo con los criterios de disponibilidad, escalabilidad, seguridad, rendimiento y capacitación administrativa de modo que se garantice el correcto funcionamiento del negocio y la proyección de crecimiento del mismo.
- La infraestructura virtualizada ayuda a las organizaciones a maximizar el valor de las inversiones tecnológicas ya que el índice de utilización de los servidores físicos es de un 80 por ciento o más (Ruest, D. Y Ruert, N., 2009).
- La principal característica que se evaluó, para tomar la decisión de utilizar la tecnología Vmware para virtualización en el Museo QCAZ, fueron los modelos de virtualización (software virtualization y hardware virtualization), en este caso Vmware utiliza el modelo hardware virtualization, el cuál se integra directamente con el hardware y lo único que hace es exponer el hardware a las máquinas virtuales, ocupando muy pocos recursos físicos del servidor dejando la mayor cantidad para las máquinas virtuales. Ayudando de esta manera a reutilizar los servidores de generaciones anteriores que dispone el Museo.
- En el caso del Museo, se puede considerar crítico que el servidor web no funcione por más de unas cuatro horas, debido a los perfiles de los usuarios que vistan el sitio web (generalmente personas vinculadas a la investigación en todo del mundo), con la infraestructura virtual la puesta en producción de un nuevo servidor no tarda más de 5 minutos.
- El sitio web del Museo QCAZ maneja una galería de fotos (22779 fotos) que guarda imágenes en alta resolución, lo que ocasiona un crecimiento extremo en la utilización del disco duro virtual, gracias a las herramientas que presenta Vmware se puede extender los discos duros virtuales en caliente.

- En redes de computadoras existe una comunicación entre diferentes equipos de computo, para que esta comunicación sea segura se deben establecer controles de seguridad que permitan proteger la información intercambiada, estos deben garantizar que se establezca la comunicación solo entre los equipos que lo requieran a través de la autenticación, además deben garantizar la protección contra el uso no autorizado de recursos, protección de los datos contra la revelación no autorizada, deben garantizar integridad de los datos y proteger cualquier tentativa de negar haber recibido o enviado datos o su contenido.
- De acuerdo al tamaño de la infraestructura del Museo QCAZ, al número de usuarios externos que se conectan al servidor actualmente y al tráfico que circula por la red, se llegó a concluir que para garantizar la seguridad de los datos se puede usar una pasarela de red (Network Gateway) configurada por software, en el caso del Museo se empleará Untangle que está recomendada para pequeñas y medianas empresas.

4.2. Recomendaciones

- Tomando en cuenta el crecimiento de los equipos tecnológicos (servidores, UPS) y de los servicios, que el Museo esta experimentando en los últimos tiempos, será necesario a mediano plazo la construcción de un data center óptimo, para esto se recomienda seguir la guía “Cómo diseñar un Data Center Óptimo” que se encuentra en el capítulo 2 del presente trabajo.
- Para montar la infraestructura virtualizada del Museo, se recomienda usar el hypervisor de VMware vSphere ESXi, luego de haber realizado un estudio comparativo se puede llegar a la conclusión que la mejor opción para la infraestructura virtual es VMware, ya que permitirá subir el porcentaje de usabilidad del servidor a un 80 por ciento o más, permitiendo de esta manera seguir utilizando los servidores de generaciones anteriores que dispone el Museo.
- Cuando los recursos de hardware son limitados, se recomienda utilizar tecnologías de virtualización que empleen el modelo hardware virtualization, ya que no utiliza una gran cantidad de los recursos físicos del servidor.
- Establecer políticas de respaldos de las máquinas virtuales, con esto se puede levantar nuevamente un servidor en menos de 5 minutos en caso de que el anterior hubiera sido dañado.
- Tomando en cuenta que la información que publica el sitio web del Museo es accedida por investigadores en todo el mundo, se podría pensar que los sistemas serán más vulnerables a posibles atacantes externos, por lo que se recomienda instalar y configurar un mecanismo de seguridad, que permita filtrar el tráfico entrante a la red.
- Si la cantidad de usuarios que se conectan al servidor sigue en aumento como lo está actualmente, se recomienda a mediano plazo comprar un dispositivo robusto de seguridad ya que en la actualidad el firewall se ha configurado mediante software.

5. Literatura citada

Abts, D., & Kim, J. (2011). *High Performance Datacenter Networks Architectures, Algorithms, and Opportunities*. (S. E. Mark D. Hill, Ed.) (p. 99). Wisconsin.

ADC, T. (2005). Cómo diseñar un centro de datos óptimo, 12.

Aldama, M. (2012). Las normas para CPD ISO / IEC 24764, 53.

Arregoces, M., & Portolani, M. (2004). *Data Center Fundamentals*. (J. Kane, Ed.) (p. 1105). Indianapolis, USA: Wait, John.

Awad, A. I., & Hassanien, A. E. (2013). *Advances in Security of Information and Communication Networks*. (K. Baba, Ed.). Cairo, Egypt.

Barba, J., & Viteri, G. (2012). *Análisis, evaluación y propuesta de optimización del funcionamiento del Data Center de la Escuela Politécnica del Ejército utilizando las normas y estándares nacionales e internacionales de calidad*. Escuela Politécnica del Ejército. Retrieved from http://www.panelamonitor.org/media/docrepo/document/files/analisis-comparativo-de-los-procesos-productivos-y-de-costeo-de-la-produccion-de-panela-y-de-bioethanol-utilizando-c.pdf

Barroso, L. A., & Hölzle, U. (2009). *The Datacenter as a Computer an Introduction to the Design of Warehouse-Scale Machines*. (M. Mark D. Hill, University of Wisconsin, Ed.). Madison: Morgan & Claypool.

Bowen, P., & Wilson, M. (2006). Information Security Handbook : A Guide for Managers, (October).

Brustein, R., & Medved, A. (2014). Firewalls, smoke and mirrors. *arXiv Preprint arXiv:1401.1401*, (1), 1–18. Retrieved from http://arxiv.org/abs/1401.1401

Building, C. T. C. S. (2012). Standars ANSI/TIA/EIA 568-B, 62.

Chalasani, S. (2010). TIA-942 : Data Center Standards, 38.

Chappell, L., & Combs, G. (2013). *Wireshark (R) 101: Essential Skills for Network Analysis* (Segunda., p. 740). California. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:wireshark+101+essential+skills+for+network+analysis#0

Colombia, U. N. de. (2003). Guía para elaboración de políticas de seguridad, 1–13.

Córdova, D. (2012). *DATA CENTER PARA MEJORAR LA INFRAESTRUCTURA DE COMUNICACIÓN DE DATOS EN EL DEPARTAMENTO DE SISTEMAS INFORMÁTICOS Y REDES DE COMUNICACIÓN (DISIR) DE LA UNIVERSIDAD TÉCNICA DE AMBATO*. Universidad Técnica de Ambato. Retrieved from http://dedi.uta.edu.ec/wp-content/uploads/KARINAPICO.pdf

DCDA, C. S. (n.d.). Data Center.

DiMinico, C. (2007). Telecommunications Infrastructure Standard for Data Centers ANSI/TIA-942.

Febrero, B. M. (2011). Análisis de tráfico con Wireshark, 52.

Ferrer, M. (2006). *Firewalls software: Estudio, instalación, configuración de escenarios y comparativa*. Universidad Politécnica de Catalunya.

Guagalango, R., & Moscoso, P. (2011). *EVALUACIÓN TÉCNICA DE LA SEGURIDAD INFORMÁTICA DEL DATA CENTER DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO*. Escuela Poltécnica del Ejército.

Haletky, E. (2011). *VMware ESX and ESXi in the Enterprise. Planning Deployment of Virtualization Servers*. (M. Taub, Ed.) (p. 589). USA: Pearson Education.

Höfler, T., Burkert, C., & Telzer, M. (2004). Comparative Firewall Study. Retrieved from http://www.qucosa.de/fileadmin/data/qucosa/documents/4892/data/firewall_study.pdf

Kappel, J., Velte, T. J., & Velte, A. T. (2009). *Microsoft Virtualization with Hyper-V*. New York.

Langenhan, D. (2013). *VMware View Security Essentials*. USA.

Lynch, H. M. (2006). Firewall Fundamentals. *Information Systems Security*, *9*(5), 1–11. doi:10.1201/1086/43312.9.5.20001112/31374.6

Marchionni, E., & Formoso, O. (n.d.). *Virtualización con VMware* (Primera., p. 356). Buenos Aires.

Mart, D. (2011). Virtualización, *20*(3), 38. doi:10.3145/epi.2011.may.16

Nicolalde, D. (2014). *ESTUDIO COMPARATIVO DE SISTEMAS DE VIRTUALIZACIÓN Y DE SEGURIDAD. CASO DE ESTUDIO MUSEO QCAZ DE LA PUCE*. Pontificia Universidad Católica del Ecuador.

Olivares Rojas, J. C. (2009). Seguridad de la Información en general.

Pino, R. E. (2014). *Network Science and Cybersecurity*. (R. E. Pino, Ed.). New York.

Portantier, F. (2012). *Seguridad Informática* (Primera., p. 192). Dalaga.

RUEST, D., & RUEST, R. (2009). *Virtualization: A Beginner's Guide*. New York.

Scarfone, K., & Hoffman, P. (2009). Guidelines on firewalls and firewall policy: recommendations of the National Institute of Standards and Technology. *NIST Special Publication*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Guidelines+on+Firewalls+and+Firewall+Policy+Recommendations+of+the+National+Institute+of+Standards+and+Technology#0

Stagner, H., & Crookston, S. (2013). *Managing and Optimizing VMware vSphere Deployments* (p. 252). United States of America: Pearson Education.

Stine, K., & Barker, W. C. (2008). Volume II : Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, *II*(August).

Stoneburner, G., Hayden, C., & Feringa, A. (2004). Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A NIST Special Publication 800-27 Rev An Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.

TELECOMUNICACIONES, U. I. DE. (2004). Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT X.800.

TIA, S. (2005). TIA-942, (April), 148.

Viteri, S. (2013). *EVALUACIÓN TÉCNICA DE LA SEGURIDAD INFORMÁTICA DEL DATA CENTER DE LA BRIGADA DE FUERZAS ESPECIALES NO. 9 PATRIA*. Escuela Politécnica del Ejército.

Vogelmann Martínez, E. E. (2008). Políticas y modelos de seguridad.

ANEXOS

ANEXO 1 – Plan de Disertación

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

PERFIL DEL TRABAJO PREVIO A LA OBTENCION DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIÓN

TEMA:

“ESTUDIO COMPARATIVO DE SISTEMAS DE VIRTUALIZACIÓN Y DE SEGURIDAD. CASO DE ESTUDIO MUSEO QCAZ DE LA PUCE.”

DAMIÁN ANÍBAL NICOLALDE RODRÍGUEZ

Quito – 2014

Contenido

Introducción.....1

Justificación.....110

Objetivo General: 115

Objetivos Específicos: 114

Alcance: 115

Índice Tentativo. 116

Cronograma 117

Bibliografía: 119

Introducción

Un flujo ininterrumpido de innovaciones en el campo de las tecnologías de información, desde el internet hasta redes inalámbricas sigue transformando el mundo. Estas innovaciones están permitiendo la creación de nuevos productos y servicios tecnológicos como: compartir información, comunicaciones digitales, Tv digital. Muchos de estos nuevos productos y/o servicios corren sobre internet o están basados en la tecnología de internet.

Estos nuevos productos y/o servicios necesitan de una infraestructura tecnológica actual, que pueda ofrecer un soporte adecuado de tal manera que se pueda brindar un servicio eficiente, se pueda garantizar disponibilidad y continuidad en las operaciones. Para cumplir con este objetivo las empresas han invertido mucho dinero para construir un ambiente apropiado y seguro en el cual se albergan todos los servidores, equipos de telecomunicaciones y los sistemas de almacenamiento. Estos ambientes conocidos como Data Centers son considerados como el centro nervioso de toda empresa, ya que están especialmente diseñados para soportar las necesidades de escalabilidad, redundancia, balanceo de carga, respaldo de energía y seguridad.

Los Data Centers, producto de decisiones poco planificadas o producto de un crecimiento mayor al esperado, han generado, que las organizaciones cuenten con una infraestructura demasiado grande, variada y difícil de administrar. En estos tiempos donde la disponibilidad, costo y eficiencia eléctrica son características importantes, han hecho pensar seriamente en migrar servicios a plataformas más eficientes y sólidas, que permitan reducir el tamaño de los Data Center en términos de inventarios, costos y facilidad para administrarlos.

Una técnica empleada para reducir el tamaño de un Data Center en términos de inventario es la virtualización, esto es que un solo recurso físico, como un servidor, aparezca como si fuera varios recursos lógicos a la vez. Esta técnica además permite subir el índice de utilización de los servidores a un 80 por ciento o más.

Un Data Center debe estar diseñado para bridar la seguridad de la información que se almacena en su graja de servidores, ya que cuya divulgación, alteración, pérdida o destrucción no autorizada puede producir daños

importantes a la organización propietaria de la misma. Es por esto que una de las tareas fundamentales de un Data Center es el área de seguridad. Para conseguir esto hay que facilitar las soluciones en continuidad, acceso, operación, procedimientos, con la finalidad de garantizar la disponibilidad en todo momento.

Justificación

El Museo Qcaz de la PUCE con el transcurso de los años ha recopilado miles de registros de información acerca de las especies de anfibios y reptiles del Ecuador, esta información ha sido almacenada en una base de datos, que con el paso del tiempo ha ido quedando obsoleta para una adecuada gestión de la información, ya que han surgido nuevas necesidades, como por ejemplo: divulgar la información, compartirla con diferentes plataformas, administración remota de la misma.

Con estas necesidades para la gestión de la información ha ido quedando el parque tecnológico del Museo QCAZ sin la suficiente capacidad de procesamiento y almacenamiento, por esto se ha visto la necesidad de renovar y actualizarlo con equipos relativamente nuevos y con capacidades de procesamiento y almacenamiento importantes.

El poco presupuesto asignado para esto, no ha permitido comprar el número suficiente de servidores. Lo que ha obligado a buscar nuevas alternativas que permitan explotar al máximo los recursos adquiridos.

Además si se toma en cuenta que el índice de utilización de los recursos tecnológicos no supera el 10 por ciento[50], no tendría sentido seguir llenando el Data Center de equipos, cuando se podría aumentar el índice de utilización de mismos.

Con este antecedente se necesita una adecuada instalación y configuración de los servidores adquiridos por el Museo QCAZ de tal manera se pueda contar con ambientes controlados y una gestión centralizada para evitar que situaciones no deseadas provoquen pérdidas de información.

Para reducir los costos del hardware y mejorar los ratios de utilización de los servidores, la virtualización es la mejor opción, ya que se puede crear a través de software una versión virtual de algún recurso tecnológico, para el caso de este estudio es la virtualización de servidores.

Los servidores del Museo QCAZ, van a almacenar toda la información de las bases de datos de las especies del Ecuador, además permitirán divulgar la

[50] Ruest, D. Y Ruest, N., 2009

información en un portal web, compartir la misma con otras plataformas a través del Internet, la gestión remota de los servidores es otro punto muy importante que se debe tomar en cuenta para evitar la vulnerabilidad de la red a ataques externos. Estos servicios que debe brindar la nueva plataforma informática del Museo QCAZ, hacen que la información esté más vulnerable a ataques por intrusos, por tal motivo la seguridad de la información es un tema crucial dentro de esta nueva configuración.

La importancia de este proyecto radica en plantear soluciones prácticas para la implementación del Data Center, el sistema de virtualización de servidores y un mecanismo de seguridad de información lo que le permitirá al Museo QCAZ brindar los servicios antes descritos con tranquilidad y seguridad.

Antecedentes

Los Data Centers albergan los recursos críticos de computación[51] en ambientes controlados y bajo una gestión centralizada (Arregoces, M. y Portolani, M., 2004), lo que permite a las empresas garantizar una operación continua en sus actividades del negocio. Estos centros de datos deben tener la capacidad de administrar toda una gama de aplicaciones que se pueden encontrar en el mercado como: aplicaciones para fiscalización interna y de recursos humanos, e-commerce y aplicaciones business-to-business. Además un número de servidores de apoyo para las operaciones de red y aplicaciones basadas en la red como: FTP, DNS, DHCP, TFTP, sistema de archivos de red NFS, aplicaciones para telefonía Ip, streaming de vídeo a través de Ip, etc.

De acuerdo con un informe del proyecto Renewable Energy Policy Project on Energy Smart Data Centers, los Data Centers son virtuales, cada empresa tiene uno o más centros de datos. Algunos han evolucionado rápidamente para dar cabida a los diferentes entornos de aplicaciones empresariales, utilizando diferentes sistemas operativos y plataformas de hardware. La evolución se ha traducido en entornos complejos que son cada vez más costosos de administrar y mantener.

La visión general de los Data Centers para el apoyo a la infraestructura de red podría no haber cambiado lo suficientemente rápido como para ser flexible en la capacidad de redundancia en curso, la escalabilidad, la seguridad y los requisitos de gestión (Arregoces, M. y Portolani, M., 2004).

Los Data Centers son un componente esencial de la infraestructura de apoyo para los servicios de internet, el comercio digital y el sector de las comunicaciones electrónicas. El continuo crecimiento de estos sectores requiere una infraestructura fiable, porque interrupciones en los servicios digitales pueden tener consecuencias económicas importantes (Arregoces, M. y Portolani, M., 2004).

Con este antecedente se puede entender que las tareas principales de los Data Centers están ligadas con el procesamiento, la disponibilidad y seguridad de la

[51] Recursos de computación, incluyen mainframes, servicios web y de aplicaciones, servidores de archivos, de impresión, de mensajería, software de aplicación y sistemas operativos, además subsistemas de almacenamiento y la infraestructura de red.

información. Cuando se habla de servicios de internet, comercio digital, etc., es importante reconocer que la información es muy vulnerable a ataques por parte de intrusos, por esto hay que encontrar una forma de proteger la misma (seguridad de la información).

Hay tres cualidades fundamentales que deben abordarse cuando se trata de la protección de la información: confidencialidad[52], integridad[53] y disponibilidad[54] (CIA) (Lynch, H. M., 2000). Los firewall[55] son herramientas que brindan soporte sobre estas tres cualidades, ellos pueden prevenir accesos no autorizados a la información; ellos pueden prevenir cambios no autorizados de la información; ellos pueden ayudar a mantener el acceso disponible a la información (Lynch, H. M., 2000).

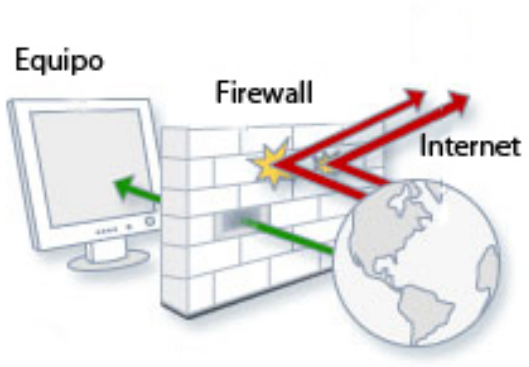


Figura 1.1 Firewall

Por otro lado, la complejidad para administrar y mantener los Data Centers, han obligado a buscar nuevas técnicas que permiten disminuir el costo de mantenimiento y administración.

Los Data Centers están cansados de correr los sistemas en servidores donde el índice de utilización es del 10 por ciento o menos (Ruest, D. Y Ruert, N., 2009), estos servidores consumen energía y requirieren un espacio y refrigeración al igual que cualquier otra máquina. Los Data Center están

[52] Confidencialidad: prevención de accesos no autorización o indeseables a la información.
[53] Integridad: asegurar que no haya cambios no autorizados sobre la información, es decir; es fiable y precisa.
[54] Disponibilidad: asegurar el acceso oportuno a la información.
[55] Firewall: Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo (Microsoft).

buscando tecnologías de virtualización[56] donde los índices de utilización de los recursos de hardware son del 80 por ciento o más (Ruest, D. Y Ruest, N., 2009), es decir, ejecutan las mismas cargas de trabajo con un hardware mucho más pequeño.

De acuerdo a Ziff-Davis Research (febrero del 2008), hay varias controladores comunes para adoptar la virtualización (vea la figura 1.2), siendo la más común la reducción de los costos del hardware y una mejora de los ratios de utilización de los servidores (Ruest, D. Y Ruest, N., 2009). No hay duda que el principal factor que impulsa la virtualización, es la virtualización de los servidores, tomando en cuenta que no es la única capa del Data Center que puede ser virtualizada.

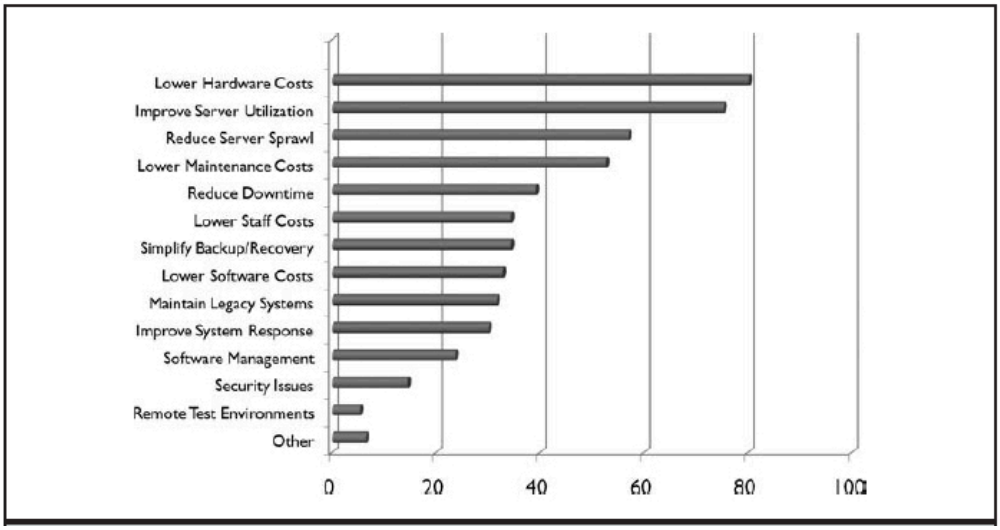


Figura 1.2 Controladores comunes de virtualización

[56] Virtualización: es la técnica empleada sobre las características físicas de algunos recursos computacionales, para ocultarlas de otros sistemas, aplicaciones o usuarios que interactúen con ellos. Esto implica hacer que un recurso físico, como un servidor, un sistema operativo o un dispositivo de almacenamiento, aparezca como si fuera varios recursos lógicos a la vez, o que varios recursos físicos, como servidores o dispositivos de almacenamiento, aparezcan como un único recurso lógico.

Objetivo General:

- Realizar un estudio de Data Centers, sistemas de virtualización y seguridad que permita implementar un sistema de virtualización y seguridad en el Museo QCAZ de la PUCE.

Objetivos Específicos:

- Analizar los protocolos que permitan una adecuada implementación de una infraestructura de Data Center.
- Realizar un análisis entre los sistemas de virtualización más utilizados y determinar cuál es la opción más adecuada para implementarla en el Museo QCAZ.
- Instalar y configurar el ambiente virtual que permitirá la configuración de todos los servidores para el Museo QCAZ.
- Diagnosticar el tráfico de la red del Museo QCAZ de tal manera que se pueda diseñar las políticas de seguridad que se implementarán en el firewall.
- Instalar y configurar el firewall para el Data Center que permita gestionar y filtrar la totalidad del tráfico entrante y saliente de nuestra red, garantizando con esto la protección de los servidores en contra de accesos no deseados de intrusos que podrían ocasionar daños físicos y lógicos permitiendo asegurar la confidencialidad, integridad y disponibilidad de la información del Museo QCAZ.

Alcance:

- El trabajo culminará con un documento de análisis acerca de los Data Centers, sistemas de virtualización, seguridad de la información y la implementación de un sistema de virtualización y un firewall en los servidores del Museo QCAZ de la PUCE.

Índice Tentativo.

Capítulo 1: Fundamentación Teórica

1. Data Centers.
    a. Introducción a la granja de servidores
    b. Protocolos de la granja de servidores
    c. Protocolos de infraestructura
2. Virtualización.
    a. Arquitectura para virtualización
    b. Construir una infraestructura de virtualización
    c. Beneficios
3. Seguridad de la información
    a. Seguridad de redes
    b. Datos y seguridad de la información
    c. Autenticación y privacidad
    d. Seguridad de aplicaciones

Capítulo 2: Metodología

1. Implementación del Data Center
2. Análisis comparativo entre sistemas de virtualización.
3. Diagnóstico del tráfico de la red con Wireshark
4. Formas para implementar un Firewall

Capítulo 3: Aplicaciones

1. Instalación y configuración del sistema de virtualización.
2. Instalación y configuración de los servidores para el Museo QCAZ
3. Instalación y configuración de un firewall.

CONCLUSIONES Y RECOMENDACIONES

BIBLIOGRAFÍA

ANEXOS

Cronograma

ACTIVIDADES	Junio				Julio				Agosto				Septiembre			
	S 1	S 2	S 3	S 4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
INTRODUCCIÓN																
CAPÍTULO 1: MARCO TEÓRICO																
1 Data center																
1.1 Introducción a la granja de servidores																
1.2 Protocolos																
2. Virtualización																
2.1. Arquitectura para virtualización																
2.2. Construir una infraestructura de virtualización																
3. Seguridad de la Información																
3.1. Seguridad de redes																
3.2. Datos y seguridad de la información																
CAPÍTULO 2: METODOLOGÍA																
1. Protocolos para la implementación del Data Center																
2. Análisis comparativo entre los sistemas de virtualización más usados en el mercado.																
3. Formas para implementar un Firewall																
CAPÍTULO 3: APLICACIONES																
1. Instalación y configuración del sistema de virtualización.																

2. Instalación y configuración de un firewall.
CONCLUSIONES
RECOMENDACIONES

Bibliografía:

Libros

CONSULINTEL, F. I. (n.d.). *FORO IPv6. CONSULINTEL*. From FORO IPv6. CONSULINTE
http://www.consulintel.es/html/ForoIPv6/RFCs.htm

Force, R. 1. (n.d.). *RFC 1924. Internet Engineering Task Force*. From RFC 1924. Inter
Task Force: http://www.ietf.org/rfc/rfc1924.txt

SOPORTE, I. 6. (n.d.). *IPv6. 6SOS: SERVICIO DE INFORMACIÓN Y SOPORTE*. From IPv
SERVICIO DE INFORMACIÓN Y SOPORTE: http://www.6sos.net/pdf/introduccion_a

SUPPORT, I. I.-I. (n.d.). *INTRODUCCIÓN IPv6. 6DEPLOY - IPV6 DEPLOYMENT AND SU*
INTRODUCCIÓN IPv6. 6DEPLOY - IPV6 DEPLOYMENT AND SUPPORT:
http://www.6deploy.eu/workshops/20090511_lima_peru/lima_introduccion_ipv6

AVANZADA, I. R. (n.d.). *IPv6. RED NICARAGUENSE DE INTERNET AVANZADA*. From I
NICARAGUENSE DE INTERNET AVANZADA: http://www.renia.net.ni/documentos/IF

J. Tatuya, S. K. *IPv6 Core Protocols Implementation.*

Blanchet, M. *Migrating to IPV6 England.*

Loshin, P. *IPV6: Theory, protocol and practice.*

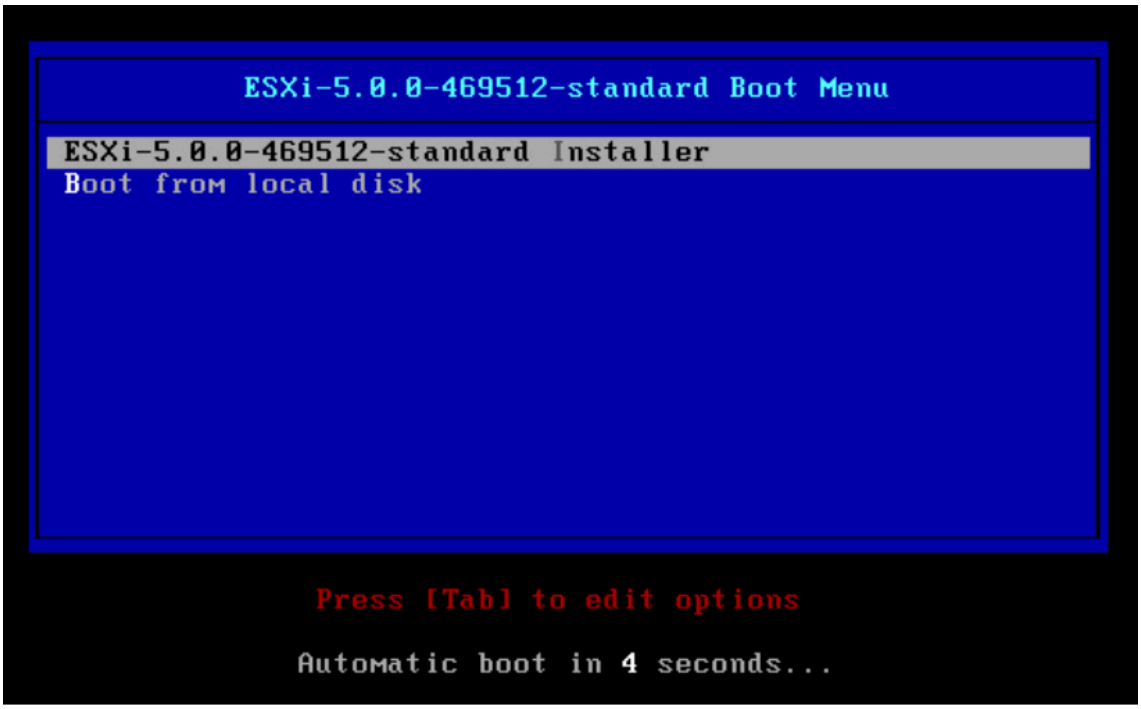
LACNIC, I. (2010). *Distribuciones/Asignaciones IPv4, espacio disponible y pronóstico*

Everything you need to know about IPv6. (I. Beijnum).

A. Conta, S. D. *Especificaciones genéricas de tunelización de paquetes en IPv6.*

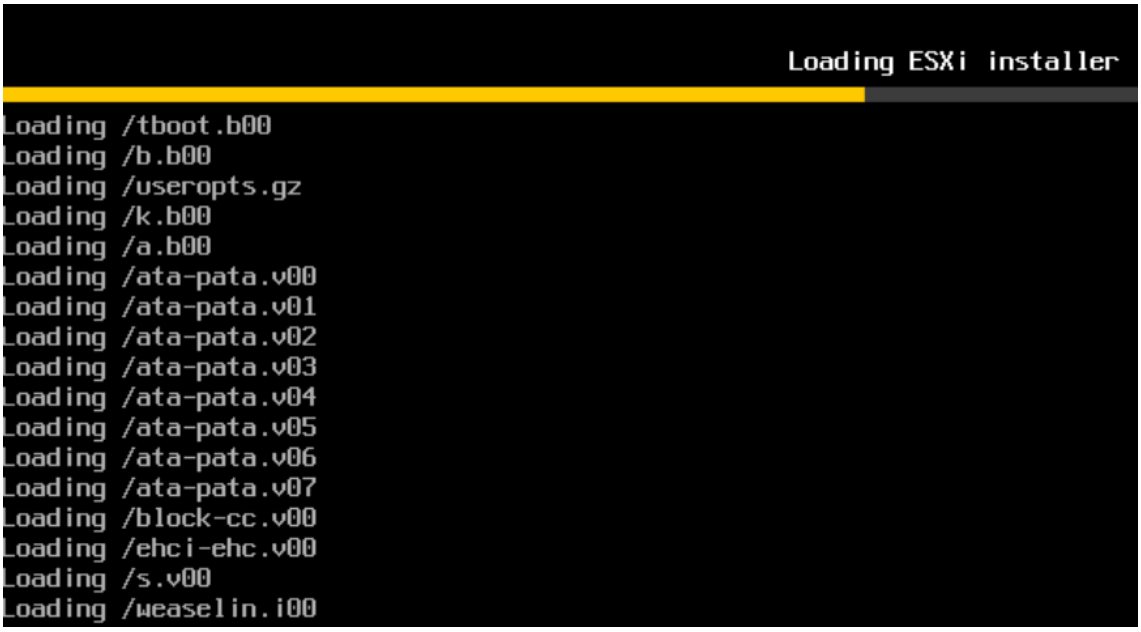
ANEXO 2 – Instalación paso a paso de VMware vSphere ESXi 5[57]

Luego de bootear el cd de instalación del VMware, aparece la pantalla que se muestra a continuación, la primera opción indica que va a cargar el sistema para instalarlo.

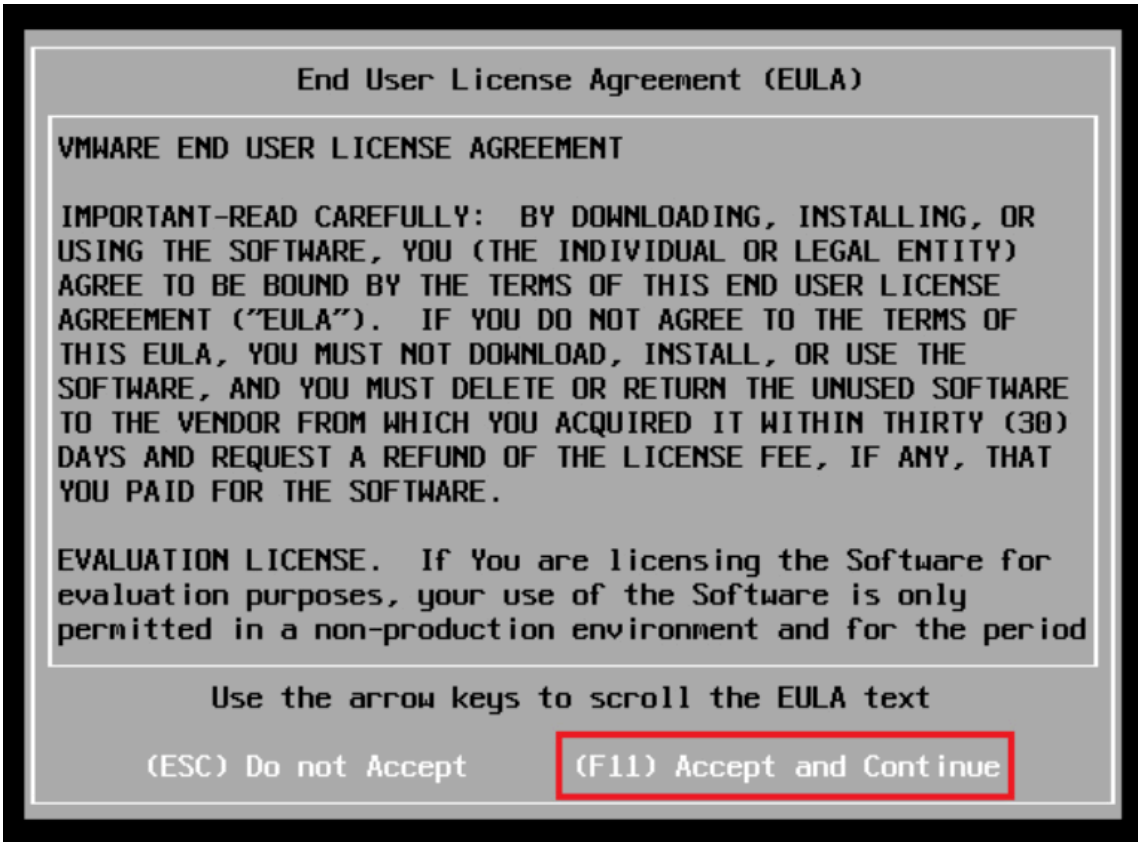


Luego de seleccionar la opción por defecto, empiezan a cargarse todos los módulos para la instalación del vSphere.

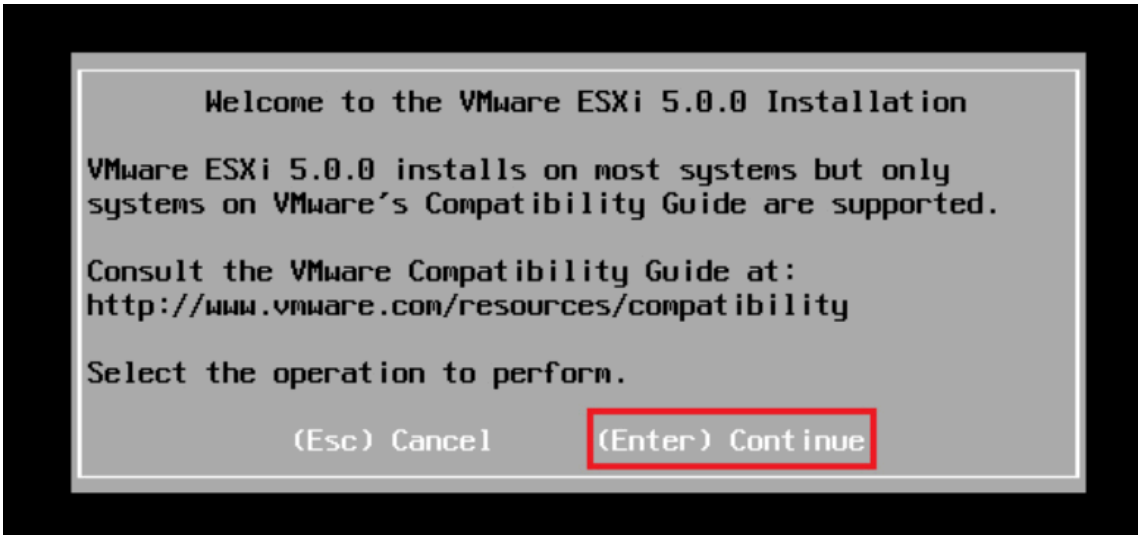
[57] Las imágenes fueron tomadas de http://www.ymant.com/es/blog/instalacion-paso-a-paso-de-vmware-vsphere-esxi-5, accedido el 11 de noviembre de 2014



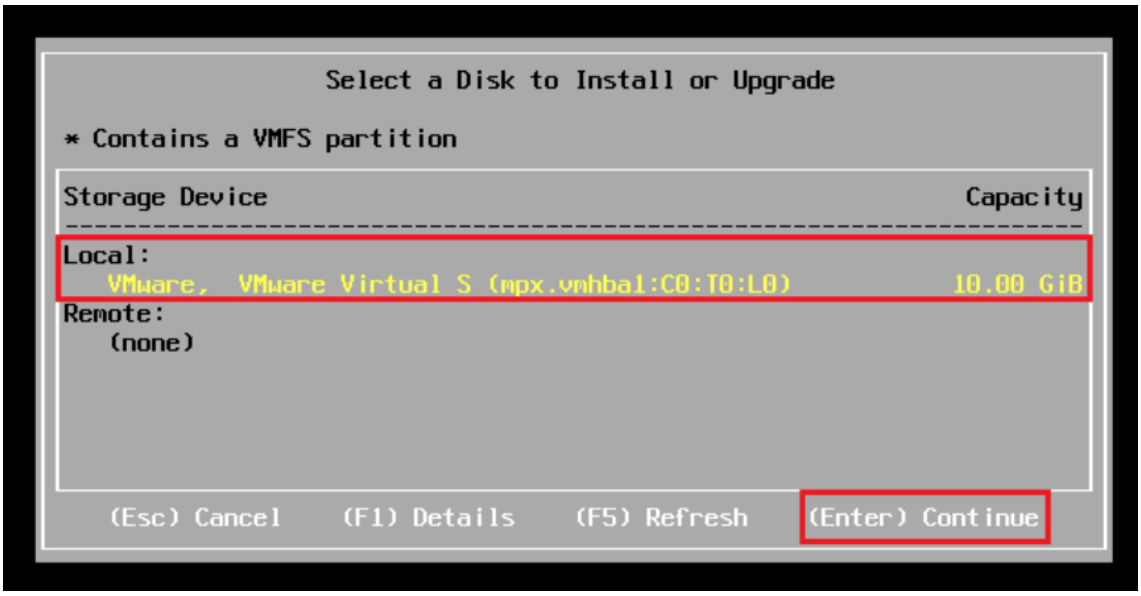
Después de cargarse los módulos, aparecen los términos de la licencia, los cuales deben ser aceptados para continuar con la instalación.



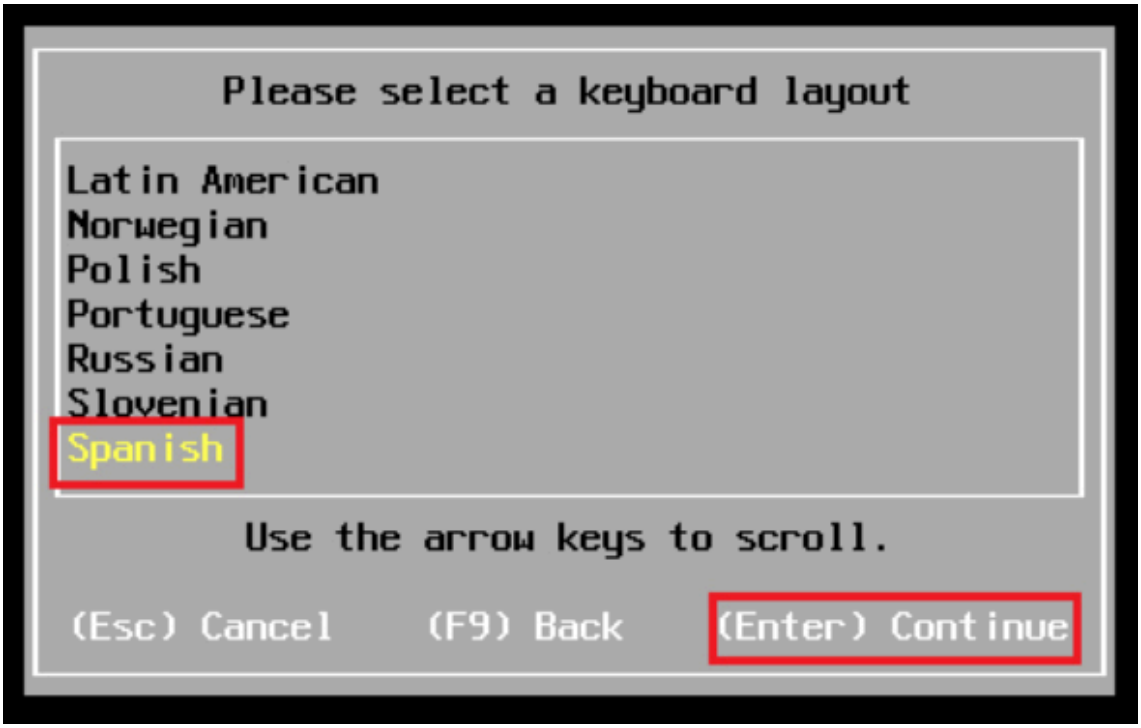
A continuación el instalador nos muestra un mensaje de bienvenida y sugiere se revise la compatibilidad del hardware.



Luego, en la pantalla siguiente se muestra el asistente de discos duros, donde hay que seleccionar el disco o arreglo de discos donde se va a instalar el vSphere.

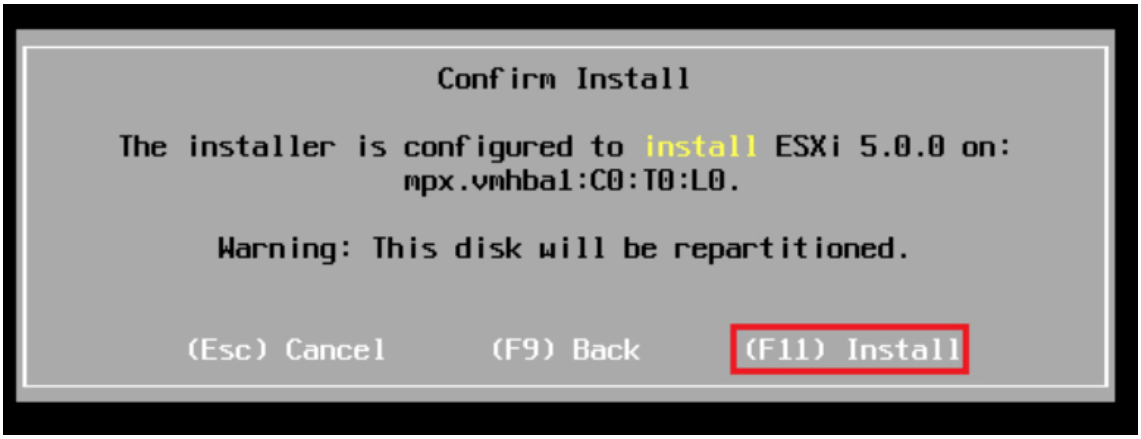


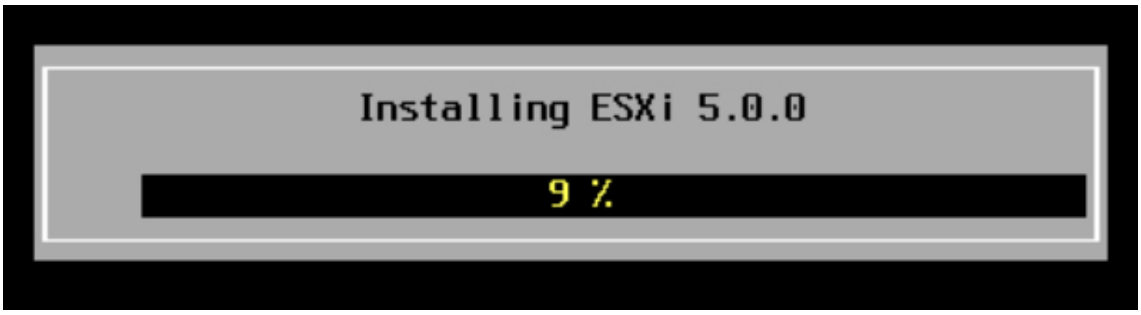
Seguidamente hay que seleccionar el idioma del teclado.



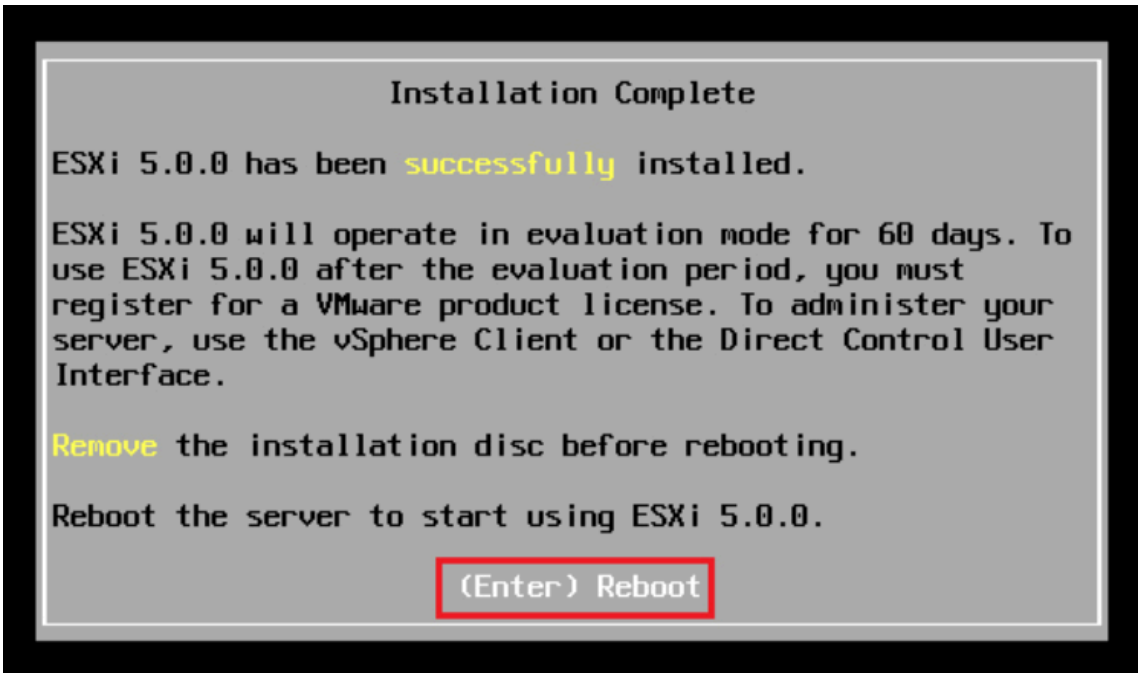
A continuación hay que escribir el password del root. De acuerdo a los requerimientos de seguridad este debe tener un mínimo de 7 caracteres.

Finalmente hay que confirmar la instalación presionando la tecla F11.





Al terminar la instalación hay que reiniciar el equipo.



Después de reiniciarse se muestra la pantalla que permite configurar el hypervisor ESXi 5.


VMware ESXi 5.0.0 (VMKernel Release Build 469512)
VMware, Inc. VMware Virtual Platform
Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz
4 GiB Memory
Download tools to manage this host from:
http://192.168.1.136/ (DHCP)
<F2> Customize System/View Logs
<F12> Shut Down/Restart